GuardDuty Amazon-Benutzerhandbuch

Amazon GuardDuty



Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon GuardDuty: GuardDuty Amazon-Benutzerhandbuch

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und die Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was ist GuardDuty? ... 1
Eigenschaften von GuardDuty ... 2
Compliance mit PCI DSS ... 7
Preisgestaltung in GuardDuty ... 7
Nutzen Sie die kostenlose GuardDuty 30-Tage-Testversion ... 8
Verwenden des Malware-Schutzes für S3 mit kostenlosem Kontingent ... 10
Zugreifen GuardDuty ... 10
Konzepte und Schlüsselbegriffe ... 12
Erste Schritte ... 18
Bevor Sie beginnen ... 18
Schritt 1: Amazon aktivieren GuardDuty ... 21
Schritt 2: Beispiel-Erkenntnisse generieren und die grundlegenden Abläufe erkunden ... 23
Schritt 3: Konfigurieren Sie den Export von GuardDuty Ergebnissen in einen Amazon S3 S3-Bucket ... 24
Schritt 4: Richten Sie die GuardDuty Suche nach Benachrichtigungen über SNS ein ... 30
Nächste Schritte ... 33
Grundlegende Datenquellen ... 34
AWS CloudTrail Verwaltungsereignisse ... 34
Wie GuardDuty geht man mit AWS CloudTrail globalen Ereignissen um ... 35
VPC Flow Logs ... 36
Route53 Resolver DNS-Abfrageprotokolle ... 37
Erweiterte Bedrohungserkennung ... 38
Beispiele für Bedrohungsszenarien mit Angriffssequenz ... 38
So funktioniert Extended Threat Detection ... 39
Aktivierung von Schutzplänen zur Maximierung der Bedrohungserkennung ... 41
Erkennung von Angriffssequenzen in Amazon EKS-Clustern ... 41
Erkennung von Angriffssequenzen in Amazon S3 S3-Buckets ... 43
Erkennung von Angriffssequenzen in Amazon ECS-Clustern ... 43
Erkennung von Angriffssequenzen in Amazon EC2 EC2-Instanzgruppen ... 44
Erweiterte Bedrohungserkennung in der Konsole GuardDuty ... 44
Die Ergebnisse der Angriffssequenz verstehen und verwalten ... 45
Weitere Ressourcen ... 45
Schutzpläne ... 47
-Übersicht ... 47

Konfiguration aller Schutzpläne ... 48
Auto-enable Optionen ... 48
Konfiguration der Laufzeitüberwachung ... 49
Bidirektionale Einschränkungen ... 49
Statistiken zur Organisation ... 50
Integration der Kontoseite ... 50
KI-Schutz ... 51
So funktioniert der KI-Schutz ... 52
Preisgestaltung für KI-Schutz ... 53
Zusätzliche Bedrohungserkennung für KI-Workloads ... 54
Aktivierung des KI-Schutzes in Umgebungen mit mehreren Konten ... 54
KI-Schutz für ein eigenständiges Konto aktivieren ... 59
EKS-Schutz ... 61
Das EKS-Audit protokolliert in EKS Protection ... 62
EKS-Schutz in Umgebungen mit mehreren Konten aktivieren ... 63
EKS-Schutz für ein eigenständiges Konto aktivieren ... 70
S3-Schutz ... 72
AWS CloudTrail Datenereignisse für S3 ... 73
Wie GuardDuty werden CloudTrail Datenereignisse für S3 verwendet ... 73
GuardDuty Verwendung von CloudTrail Datenereignissen für S3 für Angriffssequenzen ... 74
S3-Schutz in Umgebungen mit mehreren Konten aktivieren ... 75
S3-Schutz für ein eigenständiges Konto aktivieren ... 82
Laufzeitüberwachung ... 84
Funktionsweise ... 85
Mit Amazon EKS-Clustern ... 87
Mit Amazon EC2-Instanzen ... 92
Mit Fargate (nur Amazon ECS) ... 95
Nachdem Sie Runtime Monitoring aktiviert haben ... 98
Kostenlose 30-Tage-Testversion ... 99
Ich verwende den GuardDuty Testzeitraum oder habe EKS Runtime Monitoring noch nie aktiviert ... 100
Ich habe EKS Runtime Monitoring vor dem Start von Runtime Monitoring aktiviert ... 101
Voraussetzungen ... 102
Für die EC2-Instanz ... 102
ECS-EC2Für Bottlerocket ... 107
Für Fargate-Cluster (nur ECS) ... 112

Für EKS-Cluster ... 118
Laufzeitüberwachung aktivieren ... 123
Aktivierung von Runtime Monitoring für Umgebungen mit mehreren Konten ... 123
Runtime Monitoring für ein eigenständiges Konto aktivieren ... 126
Verwaltung der GuardDuty Sicherheitsagenten ... 127
Automatisierter Agent auf der Amazon EC2-Ressource ... 128
Manuelle Agentenverwaltung für Amazon EC2-Ressourcen ... 141
Automatisierter Agent auf der Bottlerocket-Ressource ECS-EC2 ... 158
Ressource „Automatisierter Agent auf Fargate“ (nur Amazon ECS) ... 159
Automatisierter Agent auf der Amazon EKS-Ressource ... 195
Manuelle Agentenverwaltung für den Amazon EKS-Cluster ... 236
Konfigurieren Sie EKS-Add-On-Parameter ... 245
Validierung der VPC-Endpunktkonfiguration ... 249
Probleme mit der Laufzeitabdeckung und Problembehandlung ... 251
Abdeckung und Problembehandlung für Amazon EC2-Ressourcen ... 252
Support und Problembehandlung für Bottlerocket ECS-EC2 ... 269
Abdeckung und Fehlerbehebung für Amazon ECS-Cluster ... 277
Abdeckung und Problembehandlung für Amazon EKS-Cluster ... 295
Einrichten der CPU- und Arbeitsspeicherüberwachung ... 312
Verwenden einer gemeinsam genutzten VPC ... 313
Funktionsweise ... 314
Voraussetzungen ... 316
Verwendung von IaC mit automatisierten Agenten ... 317
Überblick über das Diagramm zur Abhängigkeit von IaC-Ressourcen ... 317
Häufiges Problem — Löschen von Ressourcen in IaC ... 318
Gesammelte Laufzeit-Ereignistypen ... 319
Ereignisse verarbeiten ... 320
Container-Ereignisse ... 322
AWS Fargate Aufgabenereignisse (nur Amazon ECS) ... 323
Kubernetes-Pod-Ereignisse ... 324
DNS-Ereignisse (Domain Name System) ... 324
Offene Ereignisse ... 325
Lastmodul-Ereignis ... 325
Mprotect-Ereignisse ... 326
Mount-Ereignisse ... 326
Verknüpfungs-Ereignisse ... 327

Symlink-Ereignisse ... 327
Dup-Ereignisse ... 327
Arbeitsspeicherzuordnungs-Ereignis ... 328
Socket-Ereignisse ... 328
Verbindungs-Ereignisse ... 329
Prozess-VM-Readv-Ereignisse ... 330
Prozess-VM-Writev-Ereignisse ... 330
Process Trace (Ptrace) -Ereignisse ... 331
Ereignisse binden ... 332
Ereignisse anhören ... 332
Ereignisse umbenennen ... 333
Legen Sie Benutzer-ID-Ereignisse (UID) fest ... 333
Chmod-Ereignisse ... 334
Amazon ECR-Repository-Hosting-Agent GuardDuty ... 334
ECR-Repo für EKS v1.16.0 - 1.8.1 (eks.build.2) ... 335
ECR-Repo für die EKS-Version `1.8.1.eks.build.1` ... 340
ECR-Repository für Sicherheitsagenten aktiviert AWS Fargate (nur Amazon ECS) ... 342
ECR-Repository für den Sicherheitsagenten auf Bottlerocket ECS-EC2 ... 346
Security Agents auf demselben Host ... 350
-Übersicht ... 351
Auswirkung ... 351
Wie GuardDuty geht man mit mehreren Agenten um ... 351
EKS-Laufzeit-Überwachung ... 352
Konfiguration von EKS Runtime Monitoring für Umgebungen mit mehreren Konten (API) ... 353
Konfiguration von EKS Runtime Monitoring für ein eigenständiges Konto (API) ... 396
Migrieren von EKS Runtime Monitoring zu Runtime Monitoring ... 403
GuardDuty Release-Versionen des Security Agents ... 408
Zusätzliche Ressourcen — nächste Schritte ... 448
Deaktivierung, Deinstallation und Bereinigung der Ressourcen ... 448
Manuelles Deinstallieren des Security Agents für Amazon EC2-Ressourcen ... 450
Der Security Agent für ECS-EC2 Bottlerocket-Ressourcen wird deinstalliert ... 452
Bereinigen der Ressourcen des Security Agents ... 453
Malware-Schutz für EC2 ... 455
Vergleich von GuardDuty-initiated Malware-Scan und On-demand Malware-Scan ... 456
Wie werden EBS-Volumes zur Erkennung von Schadsoftware GuardDuty gescannt ... 459
Unterstützte EBS-Volumes ... 460

Ändern Sie die Standard-KMS-Schlüssel-ID ... 461
Richten Sie die Snapshot-Aufbewahrung und die EC2-Scanabdeckung ein ... 462
Snapshot-Beibehaltung ... 463
Scan-Optionen mit benutzerdefinierten Tags ... 464
Globales `GuardDutyExcluded`-Tag ... 469
GuardDuty-initiated Malware-Scan ... 469
Kostenlose 30-Tage-Testversion ... 470
Aktivierung des GuardDuty-initiated Malware-Scans in Umgebungen mit mehreren Konten . 471
Aktivierung des GuardDuty-initiated Malware-Scans für ein eigenständiges Konto ... 482
Ergebnisse, die den GuardDuty-initiated Malware-Scan auslösen ... 484
On-demand Schadsoftware scannen ... 486
So funktioniert der On-demand Malware-Scan ... 487
Der On-demand Malware-Scan wird gestartet ... 488
Re-scanning zuvor gescannte Amazon EC2-Instance ... 491
Überwachen von Scanstatus und Ergebnissen ... 491
GuardDuty Dienstkonto ... 493
Kontingente im Malware-Schutz für EC2 ... 496
Malware-Schutz für S3 ... 501
Preise und Nutzungskosten ... 503
Überprüfung der Nutzungskosten ... 505
Funktionsweise ... 505
-Übersicht ... 505
IAM-Rollenberechtigungen ... 505
Optionales Markieren von Objekten auf der Grundlage des Scanergebnisses ... 506
Vorgang, nachdem Sie Malware Protection for S3 für einen Bucket aktiviert haben ... 507
Funktionen des Malware-Schutzes für S3 ... 509
(Optional) Erste Schritte mit Malware Protection nur für S3 (Konsole) ... 510
Konfiguration des Malware-Schutzes für S3 für Ihren Bucket ... 511
Aktivieren Sie den Malware-Schutz für die S3-Bedrohungserkennung für Ihren Bucket ... 512
IAM-Rollenberechtigungen ... 519
Behebung eines Fehlers mit IAM-Rollenberechtigungen ... 524
Schritte nach der Aktivierung von Malware Protection for S3 ... 525
On-demand S3-Malware-Scan ... 527
Voraussetzungen ... 527
Starten Sie den Malware-Scan auf Abruf ... 527
Verwenden der tagbasierten Zugriffskontrolle (TBAC) ... 528

TBAC zur S3-Bucket-Ressource hinzufügen ... 529
Den Status des geschützten Buckets anzeigen und verstehen ... 531
Überwachung von S3-Objektscans ... 532
Status des potenziellen Scans und Status der Ergebnisse des S3-Objekts ... 533
Amazon verwenden EventBridge ... 537
Verwendung von S3-Objekt-Tags ... 547
Verwendung von CloudWatch Alarmen und Metriken ... 548
Fehlerbehebung ... 551
Fehlerbehebung beim Status des Malware-Schutzplans ... 551
Problembehebung bei Malware-Scan auf Abruf ... 555
Malware-Schutzplan für einen geschützten Bucket bearbeiten ... 555
Malware-Schutz für S3 für einen geschützten Bucket deaktivieren ... 557
Unterstützbarkeit der Amazon S3 S3-Funktionen ... 559
Malware-Schutz für S3-Kontingente ... 567
Malware-Schutz für AWS Backups ... 570
-Übersicht ... 570
Funktionsweise ... 573
-Übersicht ... 570
Für das Scannen ist eine IAM-Rolle erforderlich ... 575
Status und Ergebnis des Ressourcenscans werden überprüft ... 575
Überprüfung der generierten Ergebnisse ... 575
Berechtigungen für IAM-Rollen ... 577
Für das Scannen von Schadsoftware ist eine Kundenrolle vorgesehen ... 577
Einzelheiten zu den Berechtigungen ... 577
Sicherung der Rolle ... 578
So verwendet der GuardDuty Malware-Schutz Zuschüsse in AWS KMS ... 578
GuardDuty Schutz vor Schadsoftware, Verschlüsselungskontext ... 579
Berechtigungen und Vertrauensrichtlinien für die Rolle ... 580
Legen Sie unabhängig los ... 584
Schritte für die ersten Schritte mit Malware Protection for Backup ... 584
Scans auf Anforderung starten ... 585
Konsole ... 585
API/CLI ... 586
Überwachen von Scanstatus und Ergebnissen ... 586
Schutz vor Schadsoftware für Backup-Kontingente ... 595
RDS Protection ... 599

Unterstützte Datenbanken ... 601
RDS-Anmeldeaktivität ... 602
Aktivierung von RDS Protection in Umgebungen mit mehreren Konten ... 603
RDS Protection für ein eigenständiges Konto aktivieren ... 610
Behebung von Problemen bei der Überwachung von RDS Protection ... 611
RDS-Speicher voll ... 611
Nicht unterstützte Versionen der Primärdatenbank für RDS for PostgreSQL ... 612
Zusätzliche Sicherheitsüberlegungen ... 612
Lambda Protection ... 613
Lambda Network Activity Monitoring ... 614
Lambda-Schutz in Umgebungen mit mehreren Konten aktivieren ... 614
Lambda Protection für ein eigenständiges Konto aktivieren ... 622
Untersuchung — Vorschau ... 624
Arten der Analyse ... 624
Cross-Region Folgerung ... 625
Voraussetzungen ... 626
Zugriffsmodell für Administrator- und Mitgliedskonten ... 628
Eine Untersuchung erstellen ... 628
Untersuchungsergebnisse anzeigen ... 631
Interpretation der Untersuchungsergebnisse ... 633
Ermittlungen auflisten ... 634
Mehrere Konten in GuardDuty ... 637
Beziehungen zwischen Administratorkonto und Mitgliedskonto ... 638
Beziehungsstatus eines Mitglieds ... 643
Verwalten von Konten mit AWS Organizations ... 644
Überlegungen und Empfehlungen ... 645
Für die Benennung eines delegierten GuardDuty Administratorkontos sind Berechtigungen erforderlich ... 647
Benennen eines delegierten Administratorkontos GuardDuty ... 648
Einstellungen für die automatische Aktivierung von Organisationen festlegen ... 650
Mitglieder zur Organisation hinzufügen ... 654
(Optional) Aktivieren Sie Schutzpläne für bestehende Mitgliedskonten ... 657
Kontinuierliche Verwaltung Ihrer Mitgliedskonten innerhalb GuardDuty ... 658
Sperrung GuardDuty für Mitgliedskonto ... 659
Mitgliedskonto vom Administratorkonto trennen (entfernen) ... 661
Mitgliedskonten aus der GuardDuty Organisation löschen ... 663

Das delegierte GuardDuty Administratorkonto ändern ... 664
Verwalten von Konten auf Einladung ... 667
Konten auf Einladung hinzufügen ... 668
Konsolidierung von Administratorkonten unter einer einzigen Organisation ... 673
GuardDuty Überlegungen zur Option „CSV exportieren“ in Konten ... 676
Erkenntnistypen ... 677
EC2-Erkenntnistypen ... 677
Backdoor:EC2/C&CActivity.B ... 679
Backdoor:EC2/C&CActivity.B!DNS ... 680
Backdoor:EC2/DenialOfService.Dns ... 681
Backdoor:EC2/DenialOfService.Tcp ... 682
Backdoor:EC2/DenialOfService.Udp ... 682
Backdoor:EC2/DenialOfService.UdpOnTcpPorts ... 683
Backdoor:EC2/DenialOfService.UnusualProtocol ... 684
Backdoor:EC2/Spambot ... 684
Behavior:EC2/NetworkPortUnusual ... 685
Behavior:EC2/TrafficVolumeUnusual ... 686
CryptoCurrency:EC2/BitcoinTool.B ... 686
CryptoCurrency:EC2/BitcoinTool.B!DNS ... 687
DefenseEvasion:EC2/UnusualDNSResolver ... 688
DefenseEvasion:EC2/UnusualDoHActivity ... 688
DefenseEvasion:EC2/UnusualDoTActivity ... 689
Impact:EC2/AbusedDomainRequest.Reputation ... 689
Impact:EC2/BitcoinDomainRequest.Reputation ... 690
Impact:EC2/MaliciousDomainRequest.Reputation ... 691
Impact:EC2/MaliciousDomainRequest.Custom ... 691
Impact:EC2/PortSweep ... 692
Impact:EC2/SuspiciousDomainRequest.Reputation ... 692
Impact:EC2/WinRMBruteForce ... 693
Recon:EC2/PortProbeEMRUnprotectedPort ... 694
Recon:EC2/PortProbeUnprotectedPort ... 694
Recon:EC2/Portscan ... 695
Trojan:EC2/BlackholeTraffic ... 696
Trojan:EC2/BlackholeTraffic!DNS ... 697
Trojan:EC2/DGADomainRequest.B ... 697
Trojan:EC2/DGADomainRequest.C!DNS ... 698

Trojan:EC2/DNSDataExfiltration 699
Trojan:EC2/DriveBySourceTraffic!DNS 700
Trojan:EC2/DropPoint 700
Trojan:EC2/DropPoint!DNS 701
Trojan:EC2/PhishingDomainRequest!DNS 701
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom 702
UnauthorizedAccess:EC2/MetadataDNSRebind 702
UnauthorizedAccess:EC2/RDPBruteForce 703
UnauthorizedAccess:EC2/SSHBruteForce 704
UnauthorizedAccess:EC2/TorClient 706
UnauthorizedAccess:EC2/TorRelay 706
IAM-Erkenntnistypen 707
CredentialAccess:IAMUser/AnomalousBehavior 708
CredentialAccess:IAMUser/CompromisedCredentials 709
DefenseEvasion:IAMUser/AnomalousBehavior 710
DefenseEvasion:IAMUser/BedrockLoggingDisabled 710
Discovery:IAMUser/AnomalousBehavior 711
Exfiltration:IAMUser/AnomalousBehavior 712
Impact:IAMUser/AnomalousBehavior 713
InitialAccess:IAMUser/AnomalousBehavior 713
PenTest:IAMUser/KaliLinux 714
PenTest:IAMUser/ParrotLinux 715
PenTest:IAMUser/PentooLinux 715
Persistence:IAMUser/AnomalousBehavior 716
Policy:IAMUser/RootCredentialUsage 717
Policy:IAMUser/ShortTermRootCredentialUsage 717
PrivilegeEscalation:IAMUser/AnomalousBehavior 718
Recon:IAMUser/MaliciousIPCaller 719
Recon:IAMUser/MaliciousIPCaller.Custom 719
Recon:IAMUser/TorIPCaller 720
Stealth:IAMUser/CloudTrailLoggingDisabled 720
Stealth:IAMUser/PasswordPolicyChange 721
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B 722
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS 722
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS 724
UnauthorizedAccess:IAMUser/MaliciousIPCaller 726

UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom ... 726
UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS ... 727
UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS ... 729
UnauthorizedAccess:IAMUser/TorIPCaller ... 730
Arten der Suche nach Angriffssequenzen ... 731
AttackSequence:EKS/CompromisedCluster ... 732
AttackSequence:ECS/CompromisedCluster ... 733
AttackSequence:EC2/CompromisedInstanceGroup ... 734
AttackSequence:IAM/CompromisedCredentials ... 735
AttackSequence:S3/CompromisedData ... 736
S3-Schutztypen finden ... 736
Discovery:S3/AnomalousBehavior ... 738
Discovery:S3/MaliciousIPCaller ... 739
Discovery:S3/MaliciousIPCaller.Custom ... 739
Discovery:S3/TorIPCaller ... 740
Exfiltration:S3/AnomalousBehavior ... 741
Exfiltration:S3/MaliciousIPCaller ... 741
Impact:S3/AnomalousBehavior.Delete ... 742
Impact:S3/AnomalousBehavior.Permission ... 743
Impact:S3/AnomalousBehavior.Write ... 744
Impact:S3/MaliciousIPCaller ... 745
PenTest:S3/KaliLinux ... 745
PenTest:S3/ParrotLinux ... 746
PenTest:S3/PentooLinux ... 746
Policy:S3/AccountBlockPublicAccessDisabled ... 747
Policy:S3/BucketAnonymousAccessGranted ... 748
Policy:S3/BucketBlockPublicAccessDisabled ... 749
Policy:S3/BucketPublicAccessGranted ... 749
Stealth:S3/ServerAccessLoggingDisabled ... 750
UnauthorizedAccess:S3/MaliciousIPCaller.Custom ... 751
UnauthorizedAccess:S3/TorIPCaller ... 751
Arten der Suche nach EKS-Schutz ... 752
CredentialAccess:Kubernetes/MaliciousIPCaller ... 754
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom ... 755
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess ... 755
CredentialAccess:Kubernetes/TorIPCaller ... 756

DefenseEvasion:Kubernetes/MaliciousIPCaller ... 757
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom ... 758
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess ... 758
DefenseEvasion:Kubernetes/TorIPCaller ... 759
Discovery:Kubernetes/MaliciousIPCaller ... 760
Discovery:Kubernetes/MaliciousIPCaller.Custom ... 761
Discovery:Kubernetes/SuccessfulAnonymousAccess ... 762
Discovery:Kubernetes/TorIPCaller ... 762
Execution:Kubernetes/ExecInKubeSystemPod ... 763
Impact:Kubernetes/MaliciousIPCaller ... 764
Impact:Kubernetes/MaliciousIPCaller.Custom ... 765
Impact:Kubernetes/SuccessfulAnonymousAccess ... 765
Impact:Kubernetes/TorIPCaller ... 766
Persistence:Kubernetes/MaliciousIPCaller ... 767
Persistence:Kubernetes/MaliciousIPCaller.Custom ... 768
Persistence:Kubernetes/SuccessfulAnonymousAccess ... 768
Persistence:Kubernetes/TorIPCaller ... 769
Policy:Kubernetes/AdminAccessToDefaultServiceAccount ... 770
Policy:Kubernetes/AnonymousAccessGranted ... 771
Policy:Kubernetes/ExposedDashboard ... 771
Policy:Kubernetes/KubeflowDashboardExposed ... 772
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed ... 772
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated ... 773
Execution:Kubernetes/AnomalousBehavior.ExecInPod ... 774
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer ... 775
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount ... 776
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed ... 777
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated ... 779
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked ... 780
Bei der Laufzeitüberwachung werden Typen gefunden ... 781
CryptoCurrency:Runtime/BitcoinTool.B ... 783
Backdoor:Runtime/C&CActivity.B ... 784
UnauthorizedAccess:Runtime/TorRelay ... 785
UnauthorizedAccess:Runtime/TorClient ... 785

Trojan:Runtime/BlackholeTraffic 786
Trojan:Runtime/DropPoint 787
CryptoCurrency:Runtime/BitcoinTool.B! DNS 787
Backdoor:Runtime/C&CActivity.B! DNS 788
Trojan:Runtime/BlackholeTraffic! DNS 790
Trojan:Runtime/DropPoint! DNS 790
Trojan:Runtime/DGADomainRequest.C! DNS 791
Trojan:Runtime/DriveBySourceTraffic! DNS 792
Trojan:Runtime/PhishingDomainRequest! DNS 793
Impact:Runtime/AbusedDomainRequest.Reputation 793
Impact:Runtime/BitcoinDomainRequest.Reputation 794
Impact:Runtime/MaliciousDomainRequest.Reputation 795
Impact:Runtime/SuspiciousDomainRequest.Reputation 796
UnauthorizedAccess:Runtime/MetadataDNSRebind 797
Execution:Runtime/NewBinaryExecuted 799
PrivilegeEscalation:Runtime/DockerSocketAccessed 800
PrivilegeEscalation:Runtime/RuncContainerEscape 800
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified 802
DefenseEvasion:Runtime/ProcessInjection.Proc 802
DefenseEvasion:Runtime/ProcessInjection.Ptrace 803
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite 804
Execution:Runtime/ReverseShell 804
DefenseEvasion:Runtime/FilelessExecution 805
Impact:Runtime/CryptoMinerExecuted 806
Execution:Runtime/NewLibraryLoaded 806
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory 807
PrivilegeEscalation:Runtime/UserfaultfdUsage 808
Execution:Runtime/SuspiciousTool 809
Execution:Runtime/SuspiciousCommand 810
DefenseEvasion:Runtime/SuspiciousCommand 811
DefenseEvasion:Runtime/PtraceAntiDebugging 811
Execution:Runtime/MaliciousFileExecuted 812
Execution:Runtime/MaliciousFileExecuted.Custom 813
Execution:Runtime/SuspiciousShellCreated 814
PrivilegeEscalation:Runtime/ElevationToRoot 814
Discovery:Runtime/SuspiciousCommand 815

Persistence:Runtime/SuspiciousCommand ... 816
PrivilegeEscalation:Runtime/SuspiciousCommand ... 817
DefenseEvasion:Runtime/KernelModuleLoaded ... 818
Persistence:Runtime/SensitiveFileModified ... 819
PrivilegeEscalation:Runtime/SensitiveFileModified ... 820
DefenseEvasion:Runtime/SensitiveFileModified ... 821
Malware-Schutz für EC2-Suchtypen ... 821
Execution:EC2/MaliciousFile ... 822
Execution:ECS/MaliciousFile ... 823
Execution:Kubernetes/MaliciousFile ... 823
Execution:Container/MaliciousFile ... 824
Execution:EC2/SuspiciousFile ... 824
Execution:ECS/SuspiciousFile ... 825
Execution:Kubernetes/SuspiciousFile ... 826
Execution:Container/SuspiciousFile ... 826
Suchtyp „Malware-Schutz für S3“ ... 827
Object:S3/MaliciousFile ... 828
Malware-Schutz für Backup-Suchtypen ... 828
Execution:EC2/MaliciousFile!Snapshot ... 829
Execution:EC2/MaliciousFile!AMI ... 829
Execution:EC2/MaliciousFile!RecoveryPoint ... 830
Execution:S3/MaliciousFile!RecoveryPoint ... 830
Erkenntnistypen für RDS Protection ... 831
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin ... 831
CredentialAccess:RDS/AnomalousBehavior.FailedLogin ... 833
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce ... 834
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin ... 835
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin ... 835
Discovery:RDS/MaliciousIPCaller ... 836
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin ... 837
CredentialAccess:RDS/TorIPCaller.FailedLogin ... 837
Discovery:RDS/TorIPCaller ... 838
Lambda-Protection-Erkenntnistypen ... 839
Backdoor:Lambda/C&CActivity.B ... 839
CryptoCurrency:Lambda/BitcoinTool.B ... 840
Trojan:Lambda/BlackholeTraffic ... 841

Trojan:Lambda/DropPoint ... 841
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom ... 842
UnauthorizedAccess:Lambda/TorClient ... 842
UnauthorizedAccess:Lambda/TorRelay ... 843
Arten der Suche nach KI-Schutz ... 843
Impact:IAMUser/AnomalousModelInvocation ... 844
Impact:IAMUser/CostHarvesting ... 846
Impact:IAMUser/PromptInjection.Direct ... 847
Nicht mehr aktive Erkenntnistypen ... 849
PrivilegeEscalation:Kubernetes/PrivilegedContainer ... 851
Persistence:Kubernetes/ContainerWithSensitiveMount ... 851
Exfiltration:S3/ObjectRead.Unusual ... 852
Impact:S3/PermissionsModification.Unusual ... 853
Impact:S3/ObjectDelete.Unusual ... 853
Discovery:S3/BucketEnumeration.Unusual ... 854
Persistence:IAMUser/NetworkPermissions ... 855
Persistence:IAMUser/ResourcePermissions ... 856
Persistence:IAMUser/UserPermissions ... 857
PrivilegeEscalation:IAMUser/AdministrativePermissions ... 858
Recon:IAMUser/NetworkPermissions ... 859
Recon:IAMUser/ResourcePermissions ... 859
Recon:IAMUser/UserPermissions ... 860
ResourceConsumption:IAMUser/ComputeResources ... 861
Stealth:IAMUser/LoggingConfigurationModified ... 862
UnauthorizedAccess:IAMUser/ConsoleLogin ... 863
UnauthorizedAccess:EC2/TorIPCaller ... 863
Backdoor:EC2/XORDDOS ... 864
Behavior:IAMUser/InstanceLaunchUnusual ... 864
CryptoCurrency:EC2/BitcoinTool.A ... 865
UnauthorizedAccess:IAMUser/UnusualASNCaller ... 865
GuardDuty Suchen nach Typen anhand potenziell betroffener Ressourcen ... 866
GuardDuty Typen von aktiven Ergebnissen ... 866
Ergebnisse verstehen und generieren ... 891
GuardDuty Format finden ... 892
Bedrohungszwecke ... 894
GuardDuty Scan-Engine zur Malware-Erkennung ... 897

Beispielerkenntnisse ... 898
Generierung von Beispielergebnissen über die GuardDuty Konsole oder API ... 898
GuardDuty Testergebnisse ... 899
Überlegungen ... 900
GuardDuty Ergebnisse, die das Tester-Skript generieren kann ... 901
Schritt 1 — Voraussetzungen ... 904
Schritt 2 — Ressourcen bereitstellen AWS ... 904
Schritt 3 — Führen Sie Tester-Skripte aus ... 906
Schritt 4 — Testressourcen AWS bereinigen ... 909
Behebung häufiger Probleme ... 909
Seite mit den Ergebnissen in der GuardDuty Konsole ... 911
Auf der Seite „Ergebnisse“ navigieren ... 912
Schweregrad der Ergebnisse ... 914
Kritischer Schweregrad ... 914
Hoher Schweregrad ... 915
Mittlerer Schweregrad ... 915
Niedriger Schweregrad ... 916
Erkenntnisdetails ... 916
Überblick über Erkenntnisse ... 917
Ressource ... 918
Einzelheiten zur Suche nach der Angriffssequenz ... 925
Benutzerdetails für die RDS-Datenbank (DB) ... 934
Details zu den Erkenntnissen der Laufzeitüberwachung ... 934
Scan-Details der EBS-Volumes ... 937
Einzelheiten zur Suche nach Malware Protection for EC2 ... 938
Einzelheiten zu Erkenntnissen von Malware Protection für S3 ... 939
Action ... 940
Akteur oder Ziel ... 942
Einzelheiten zur Geolokalisierung ... 943
Zusätzliche Informationen ... 943
Beweise ... 944
Anormales Verhalten ... 944
GuardDuty Aggregation finden ... 949
Verwaltung der GuardDuty Ergebnisse ... 951
GuardDuty Übersichts-Dashboard ... 952
-Übersicht ... 953

Ergebnisse 954
Die häufigsten Arten von Erkenntnissen 955
Erkenntnisse nach Schweregrad 955
Konten mit den meisten Erkenntnissen 956
Ressourcen mit Erkenntnissen 956
Am wenigsten auftretende Erkenntnisse 957
Geltungsbereich der Schutzpläne 957
GuardDuty Ergebnisse filtern 958
Filtersatz in der GuardDuty Konsole erstellen und speichern 959
Filtersatz mithilfe von GuardDuty API und CLI erstellen und speichern 961
Lebenszyklusmetadaten 963
Eigenschaftsfilter in GuardDuty 964
Unterdrückungsregeln 997
Verwendung von Unterdrückungsregeln mit Extended Threat Detection 998
Häufige Anwendungsfälle für Unterdrückungsregeln und Beispiele 999
Unterdrückungsregeln erstellen 1002
Aktualisierung der Unterdrückungsregeln 1007
Löschen von Unterdrückungsregeln 1010
Kennzahlen für Unterdrückungsregeln 1012
Entitätslisten und IP-Adresslisten 1013
Grundlegendes zu Entitätslisten und IP-Adresslisten 1014
Wichtige Überlegungen zu GuardDuty Listen 1015
Listenformate 1016
Grundlegendes zum Listenstatus 1025
Voraussetzungen für Entitätslisten und IP-Adresslisten einrichten 1026
Hinzufügen und Aktivieren einer Entitätsliste oder IP-Liste 1028
Aktualisierung einer Entitäts- oder IP-Adressliste 1035
De-activating Entitätsliste oder IP-Adressliste 1041
Entitätsliste oder IP-Adressliste löschen 1043
Generierte Ergebnisse nach Amazon S3 exportieren 1046
Überlegungen 1047
Schritt 1 — Zum Exportieren der Ergebnisse sind Berechtigungen erforderlich 1048
Schritt 2 — Richtlinie an Ihren KMS-Schlüssel anhängen 1049
Schritt 3 — Richtlinie an den Amazon S3-Bucket anhängen 1051
Schritt 4 — Ergebnisse in einen S3-Bucket exportieren (Konsole) 1055
Schritt 5 — Häufigkeit für den Export von Ergebnissen 1056

Bearbeitung von Ergebnissen mit EventBridge 1057
EventBridge Benachrichtigungshäufigkeit in GuardDuty 1058
Ein Amazon SNS SNS-Thema und einen Endpunkt einrichten 1059
Verwenden EventBridge mit GuardDuty 1060
Erstellen einer EventBridge Regel 1062
EventBridge Regel für Umgebungen mit mehreren Konten 1069
Grundlegendes zu CloudWatch Protokollen und Gründen für das Überspringen von Ressourcen 1070
CloudWatch Audit-Protokolle in Malware Protection for EC2 GuardDuty 1070
GuardDuty Malware-Schutz für die Aufbewahrung von EC2-Protokollen 1072
Gründe für das Überspringen der Ressource 1073
Falsch positives EC2-Malware-Scanergebnis melden 1079
Falsch positives S3-Objektscanergebnis melden 1080
Falsch positives Backup-Malware-Scanergebnis melden 1081
Behebung von Erkenntnissen 1083
Behebung einer potenziell kompromittierten Amazon EC2-Instance 1083
Behebung eines potenziell kompromittierten S3-Buckets 1085
Empfehlungen, die auf spezifischen S3-Bucket-Zugriffsanforderungen basieren 1087
Behebung eines potenziell bösartigen S3-Objekts 1088
Behebung eines potenziell kompromittierten EBS-Snapshots 1089
Behebung eines potenziell kompromittierten EC2-AMI 1090
Behebung eines potenziell kompromittierten EC2-Wiederherstellungspunkts 1091
Behebung eines potenziell kompromittierten S3-Wiederherstellungspunkts 1092
Behebung eines potenziell kompromittierten ECS-Clusters 1093
Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten 1094
Behebung eines potenziell kompromittierten Standalone-Containers 1096
Behebung der EKS-Schutzfeststellungen 1097
Mögliche Konfigurationsprobleme 1098
Behebung potenziell gefährdeter Kubernetes-Benutzer 1098
Behebung potenziell kompromittierter Kubernetes-Pods 1101
Behebung potenziell kompromittierter Container-Images 1103
Behebung potenziell kompromittierter Kubernetes-Knoten 1104
Korrigieren von Erkenntnissen der Laufzeitüberwachung 1104
Behebung kompromittierter Container-Images 1106
Behebung einer potenziell gefährdeten Datenbank 1107
Behebung einer potenziell gefährdeten Datenbank mit erfolgreichen Anmeldeereignissen . 1107

Behebung einer potenziell gefährdeten Datenbank mit erfolglosen Anmeldeereignissen 1108
Behebung potenziell kompromittierter Anmeldeinformationen 1110
Einschränken von Netzwerkzugriff 1110
Behebung einer potenziell gefährdeten Lambda-Funktion 1111
Überwachung der Nutzung und Schätzung der Kosten 1112
CloudWatch Amazon-Nutzungsmetriken 1112
Angaben zur Metrik 1112
Malware-Schutz für S3 1115
Grundlegendes GuardDuty zur Nutzung 1116
GuardDuty Verarbeitung von Ereignissen 1116
GuardDuty Gebühren für die Verarbeitung von VPC Flow Logs für Instanzen, die von Runtime Monitoring überwacht werden GuardDuty 1117
Schätzung der Kosten GuardDuty 1117
Verwenden AWS Preiskalkulator 1118
Security Hub-Kunden 1119
Funktionsnamen für Schutzpläne in der API 1120
Wechseln Sie von Datenquellen zu Funktionen 1120
GuardDuty API-Änderungen 1120
Funktionen im Vergleich zu Datenquellen 1121
Verstehen, wie APIs mit Funktionen funktionieren 1121
Integration von Funktionsänderungen in APIs 1122
Zugeordnete Funktion GuardDuty 1123
Sicherheit 1126
Datenschutz 1127
Verschlüsselung im Ruhezustand 1128
Verschlüsselung während der Übertragung 1128
Abmeldung von der Verwendung Ihrer Daten zur Serviceverbesserung 1128
Protokollierung mit CloudTrail 1130
GuardDuty Informationen in CloudTrail 1130
GuardDuty Ereignisse auf der Kontrollebene in CloudTrail 1131
GuardDuty Datenereignisse in CloudTrail 1132
Beispiel: Einträge in GuardDuty Protokolldateien 1133
Identitäts- und Zugriffsverwaltung 1135
Zielgruppe 1136
Authentifizierung mit Identitäten 1136
Verwalten des Zugriffs mit Richtlinien 1138

So GuardDuty arbeitet Amazon mit IAM 1140
Identity-based Beispiele für Richtlinien 1145
Verwenden von servicegebundenen Rollen 1156
AWS verwaltete Richtlinien 1167
Fehlerbehebung 1184
Compliance-Validierung 1186
Ausfallsicherheit 1186
Sicherheit der Infrastruktur 1186
VPC-Endpunkte (AWS PrivateLink) 1187
Überlegungen zu GuardDuty VPC-Endpunkten 1187
Erstellen eines Schnittstellen-VPC-Endpunkts für GuardDuty 1187
Erstellen einer VPC-Endpunktrichtlinie für GuardDuty 1188
Gemeinsam genutzte Subnetze 1189
Integration mit AWS Sicherheitsdiensten 1190
Integration GuardDuty mit AWS Security Hub CSPM 1190
Integration GuardDuty mit Amazon Detective 1190
AWS Security Hub CSPM Integration 1190
So GuardDuty sendet Amazon Ergebnisse an AWS Security Hub CSPM 1191
Ergebnisse anzeigen in GuardDuty AWS Security Hub CSPM 1192
Aktivieren und Konfigurieren der Integration 1212
Verwendung von GuardDuty Steuerelementen in Security Hub CSPM 1212
Einstellung der Veröffentlichung der Ergebnisse im Security Hub CSPM 1212
Integration mit Amazon Detective 1213
Aktivierung der Integration 1213
Von einem GuardDuty Befund zu Amazon Detective wechseln 1214
Verwendung der Integration in einer Umgebung mit GuardDuty mehreren Konten 1214
Unterbrechen oder Deaktivieren 1216
GuardDuty Ankündigungen 1218
Amazon-SNS-Nachrichtenformat 1224
GuardDuty Kontingente 1230
Support für verwaltete Instanzen 1237
Fehlerbehebung 1238
Ergebnisse nach Amazon S3 exportieren — Zugriffsfehler 1238
Malware-Schutz bei EC2-Problemen 1239
Bei der Aktivierung des GuardDuty-initiated Malware-Scans fehlt die erforderliche AWS Organizations Verwaltungsberechtigung 1239

Ich initiiere einen On-demand Malware-Scan, der jedoch zu einem Fehler wegen fehlender erforderlicher Berechtigungen führt. 1239
Ich erhalte bei der Arbeit mit Malware Protection for EC2 eine `iam:GetRole` Fehlermeldung. 1240
Ich habe ein GuardDuty Administratorkonto, das den GuardDuty-initiated Malware-Scan aktivieren muss, aber nicht die AWS verwaltete Richtlinie verwendet: AmazonGuardDutyFullAccess zur Verwaltung GuardDuty. 1240
Probleme mit der Laufzeitüberwachung 1240
Probleme mit der Runtime-Abdeckung 1240
Behebung eines Fehlers wegen unzureichenden Speichers 1241
Mein AWS Step Functions Workflow schlägt unerwartet fehl 1241
Fehlerbehebung bei anderen Problemen 1242
Regionen und Endpunkte 1243
Region-specific Verfügbarkeit von Funktionen 1243
Ältere GuardDuty-Aktionen und -Parameter 1246
Dokumentverlauf 1248
Frühere Aktualisierungen 1355
..... mccclvi

Was ist Amazon GuardDuty?

Amazon GuardDuty ist ein Service zur Bedrohungserkennung, der kontinuierlich AWS Datenquellen und Protokolle in Ihrer AWS Umgebung überwacht, analysiert und verarbeitet. GuardDuty verwendet Threat-Intelligence-Feeds wie Listen bösartiger IP-Adressen und Domains, Datei-Hashes und Modelle für maschinelles Lernen (ML), um verdächtige und potenziell bösartige Aktivitäten in Ihrer AWS Umgebung zu identifizieren. Die folgende Liste bietet einen Überblick über potenzielle Bedrohungsszenarien, anhand derer Sie Folgendes erkennen GuardDuty können:

- Kompromittierte und exfiltrierte Anmeldeinformationen AWS .
- Exfiltration und Zerstörung von Daten, die zu einem Ransomware-Ereignis führen können. Ungewöhnliche Muster von Anmeldeereignissen in den unterstützten Engine-Versionen der Amazon Aurora- und Amazon RDS-Datenbanken, die auf ein anomales Verhalten hinweisen.
- Unautorisierte Cryptomining-Aktivitäten in Ihren Amazon Elastic Compute Cloud (Amazon EC2) -Instances und Container-Workloads.
- Vorhandensein von Malware in Ihren Amazon EC2 EC2-Instances und Container-Workloads sowie neu hochgeladene Dateien in Ihren Amazon Simple Storage Service (Amazon S3) -Buckets.
- Ereignisse auf Betriebssystemebene, Netzwerk- und Dateiereignisse, die auf unberechtigtes Verhalten in Ihren Amazon Elastic Kubernetes Service (Amazon EKS) -Clustern, Amazon Elastic Container Service (Amazon ECS) AWS Fargate -Aufgaben und Amazon EC2 EC2-Instances und Container-Workloads hinweisen.

Das folgende Video bietet einen Überblick darüber, wie Sie Bedrohungen in Ihrer Umgebung GuardDuty erkennen können. AWS

Was ist Amazon GuardDuty

Inhalt

- Eigenschaften von GuardDuty
- Compliance mit PCI DSS
- Preisgestaltung in GuardDuty
- Zugreifen GuardDuty

Eigenschaften von GuardDuty

Im Folgenden finden Sie einige der wichtigsten Methoden, mit denen Amazon GuardDuty Sie bei der Überwachung, Erkennung und Verwaltung potenzieller Bedrohungen in Ihrer AWS Umgebung unterstützen kann.

Überwacht kontinuierlich bestimmte Datenquellen und Ereignisprotokolle

- Fundamentale Bedrohungserkennung — Wenn Sie GuardDuty in an aktivieren AWS-Konto, GuardDuty werden automatisch die grundlegenden Datenquellen aufgenommen, die mit diesem Konto verknüpft sind. Zu diesen Datenquellen gehören AWS CloudTrail Verwaltungsereignisse,

VPC-Flow-Protokolle (von Amazon EC2 EC2-Instances) und DNS-Protokolle. Sie müssen nichts anderes aktivieren, um mit der Analyse und Verarbeitung dieser Datenquellen GuardDuty zu beginnen, um zugehörige Sicherheitsergebnisse zu generieren. Weitere Informationen finden Sie unter GuardDuty grundlegende Datenquellen.

- Erweiterte Bedrohungserkennung — Diese Funktion erkennt mehrstufige Angriffe, die grundlegende Datenquellen, mehrere Arten von AWS Ressourcen und Zeit innerhalb eines Zeitraums umfassen. AWS-Konto In Ihrem Konto gibt es möglicherweise mehrere Ereignisse, die für sich genommen keine eindeutige Bedrohung darstellen. Wenn diese Ereignisse jedoch in einer Reihenfolge beobachtet werden, die auf eine verdächtige Aktivität hinweist, wird dies als Angriffssequenz GuardDuty identifiziert. GuardDuty benachrichtigt Sie, indem es den zugehörigen Erkennungstyp der Angriffssequenz generiert, um Ihnen Einzelheiten zur beobachteten Angriffssequenz bereitzustellen.

  Extended Threat Detection wird AWS-Konto bei jeder Aktivierung automatisch aktiviert, ohne dass zusätzliche Kosten anfallen. GuardDuty Für diese Funktion müssen Sie keinen anwendungsspezifischen Schutzplan aktivieren. Um die Sicherheit Ihrer Amazon S3 S3-Ressourcen zu erhöhen, GuardDuty empfiehlt es sich jedoch, S3 Protection in Ihrem Konto zu aktivieren. Auf diese Weise kann Extended Threat Detection mehrstufige Angriffe identifizieren, die sich möglicherweise auf Ihre Amazon S3 S3-Ressourcen auswirken.

  Weitere Informationen darüber, wie diese Funktion funktioniert und welche Bedrohungsszenarien sie abdeckt, finden Sie unterGuardDuty Erweiterte Bedrohungserkennung.
- Untersuchung (Vorschau) — GuardDuty Investigation bietet eine AI-powered Sicherheitsanalyse Ihrer GuardDuty Ergebnisse. Sie können Untersuchungen erstellen, um bestimmte Ergebnisse, Konten oder Ihr gesamtes Unternehmen zu analysieren und anschließend strukturierte Zusammenfassungen der Untersuchungen mit Risikobeurteilung, Vertrauensbewertung, MITRE ATT&CK® -Klassifizierung und umsetzbaren nächsten Schritten zu erhalten. Weitere Informationen finden Sie unter GuardDuty Untersuchung (Vorschau).
- Use-case gezielte GuardDuty Schutzpläne — Für einen besseren Einblick in die Sicherheit Ihrer AWS Umgebung bei der Erkennung von Bedrohungen GuardDuty bieten wir spezielle Schutzpläne, die Sie aktivieren können. Schutzpläne helfen Ihnen bei der Überwachung von Protokollen und Ereignissen anderer AWS Dienste. Zu diesen Quellen gehören EKS-Auditprotokolle, RDS-Anmeldeaktivitäten, Amazon S3 S3-Datenereignisse in CloudTrail, EBS-Volumes, Runtime Monitoring in Amazon EKS, Amazon EC2 und Amazon ECS-Fargate, Lambda-Netzwerkaktivitätsprotokolle und AWS CloudTrail Datenereignisse von Amazon Bedrock, Amazon Bedrock und Amazon SageMaker AI for AI for AgentCore AI Protection.

GuardDutyfasst diese Protokoll- und Ereignisquellen unter dem Begriff „Funktionen“ zusammen. Sie können jederzeit einen oder mehrere spezielle Schutzpläne in AWS-Region einem unterstützten Paket aktivieren. GuardDuty beginnt mit der Überwachung, Verarbeitung und Analyse der Aktivitäten auf der Grundlage des von Ihnen aktivierten Schutzplans. Weitere Informationen zu den einzelnen Schutzplänen und ihrer Funktionsweise finden Sie im entsprechenden Schutzplandokument.

GuardDuty Bei der ersten Aktivierung GuardDuty werden automatisch alle Schutzpläne außer Runtime Monitoring für Ihr Konto aktiviert und in die kostenlose 30-Tage-Testversion aufgenommen. Sie können jeden Schutzplan jederzeit deaktivieren. Wenn Sie bereits GuardDuty Kunde sind, wird ein Schutzplan, der nach der Aktivierung gestartet GuardDuty wird, nicht automatisch aktiviert. Sie können ihn aber auch aktivieren. Informationen darüber, welche Schutzpläne standardmäßig aktiviert sind, finden Sie unterNutzen Sie die kostenlose GuardDuty 30-Tage-Testversion.

Schutzplan	Description
KI-Schutz	Erkennt Bedrohungen für Ihre KI-Workloads, die Amazon Bedrock, Amazon Bedrock und Amazon SageMaker AI verwenden AgentCore, wie z. B. anomale Modellaufrufe und Cost-Harvesting-Angriffe.
S3-Schutz	Identifiziert potenzielle Sicherheitsrisiken wie Datenexfi ltrations- und Zerstörungsversuche in Ihren Amazon S3 S3-Buckets.
EKS-Schutz	EKS Audit Log Monitoring analysiert Kubernetes-Auditpr otokolle aus Ihren Amazon EKS-Clustern auf potenziell verdächtige und böswillige Aktivitäten.
Laufzeitüberwachung	Überwacht und analysiert Ereignisse auf Betriebss ystemebene auf Ihrem Amazon EKS, Amazon EC2 und Amazon ECS (einschließlich AWS Fargate), um potenzielle Laufzeitbedrohungen zu erkennen.

Schutzplan	Description
Malware-Schutz für EC2	Erkennt das potenzielle Vorhandensein von Malware, indem es die Amazon EBS-Volumes scannt, die Ihren Amazon EC2 EC2-Instances zugeordnet sind. Es besteht die Möglichkeit, diese Funktion bei Bedarf zu nutzen.
Malware-Schutz für S3	Erkennt das potenzielle Vorhandensein von Malware in den neu hochgeladenen Objekten in Ihren Amazon S3 S3-Bucket s. Es besteht die Möglichkeit, diese Funktion bei Bedarf zu nutzen.
Malware-Schutz für AWS Backups	Erkennt das potenzielle Vorhandensein von Malware durch Scannen von Backup-Ressourcen, einschließlich EBS-Snapshots, EC2-AMIs und AWS Backup-Wiederherst ellungspunkten. Es besteht die Möglichkeit, diese Funktion bei Bedarf zu verwenden.
RDS Protection	Analysiert und profiliert Ihre RDS-Anmeldeaktivitäten im Hinblick auf potenzielle Zugriffsbedrohungen auf die unterstützten Amazon Aurora- und Amazon RDS-Daten banken.
Lambda Protection	Überwacht Lambda-Netzwerkaktivitätsprotokolle, beginnend mit VPC-Flussprotokollen, um Bedrohungen für Ihre AWS Lambda Funktionen zu erkennen. Zu diesen potenziellen Bedrohungen gehören beispielsweise Cryptomining und die Kommunikation mit bösartigen Servern.

Aktivieren Sie den Malware-Schutz für S3 unabhängig

GuardDuty bietet die Flexibilität, Malware Protection for S3 unabhängig zu verwenden, ohne den GuardDuty Amazon-Service zu aktivieren. Weitere Informationen zu den ersten Schritten nur mit Malware Protection for S3 finden Sie unterGuardDuty Malware-Schutz für S3. Um alle anderen Schutzpläne nutzen zu können, müssen Sie den GuardDuty Dienst aktivieren.

Verwaltung einer Umgebung mit mehreren Konten

Sie können eine AWS Umgebung mit mehreren Konten verwalten, indem Sie entweder die AWS Organizations (empfohlene) oder die herkömmliche Einladungsmethode verwenden. Weitere Informationen finden Sie unter Mehrere Konten in GuardDuty.

Generiert Sicherheitsergebnisse für erkannte Bedrohungen

Wenn potenzielle Sicherheitsbedrohungen im Zusammenhang mit Ihren AWS Ressourcen GuardDuty erkannt werden, werden Sicherheitsergebnisse generiert, die Informationen über die potenziell gefährdete Ressource liefern. Generieren Sie nach GuardDuty der Aktivierung in Ihrem Konto, Beispielerkenntnisse um die zugehörigen Erkenntnisdetails Dateien anzuzeigen. Eine vollständige Liste der Sicherheitsergebnisse finden Sie unterGuardDuty Typen finden.

Mit GuardDuty können Sie auch ein Testerskript verwenden, das spezifische GuardDuty Sicherheitserkenntnisse generiert, um zu verstehen, wie die GuardDuty Ergebnisse überprüft und darauf reagiert werden. Weitere Informationen finden Sie unter GuardDuty Testergebnisse in speziellen Konten.

Bewertung und Verwaltung von Sicherheitsergebnissen

GuardDuty konsolidiert Ihre Sicherheitsfeststellungen für alle Konten und zeigt die Ergebnisse im Übersichts-Dashboard auf der GuardDuty Konsole an. Sie können die Ergebnisse auch über die AWS Security Hub CSPM API oder das AWS Command Line Interface AWS SDK abrufen. Mit einem ganzheitlichen Überblick über Ihren aktuellen Sicherheitsstatus können Sie Trends und potenzielle Probleme erkennen und die erforderlichen Abhilfemaßnahmen ergreifen. Weitere Informationen finden Sie unter Verwaltung der GuardDuty Ergebnisse.

Integrieren Sie es in verwandte AWS Sicherheitsdienste

Um Sie bei der Analyse und Untersuchung der Sicherheitstrends in Ihrer AWS Umgebung weiter zu unterstützen, sollten Sie die folgenden AWS sicherheitsbezogenen Services in Kombination mit in Betracht ziehen. GuardDuty

- AWS Security Hub CSPM— Dieser Service bietet Ihnen einen umfassenden Überblick über den Sicherheitsstatus Ihrer AWS Ressourcen und hilft Ihnen, Ihre AWS Umgebung anhand der Sicherheitsstandards und bewährten Verfahren der Branche zu überprüfen. Dies geschieht zum Teil durch die Nutzung, Zusammenfassung, Organisation und Priorisierung Ihrer Sicherheitsergebnisse aus mehreren AWS Diensten (einschließlich Amazon Macie) und unterstützten AWS Partner Network (APN) -Produkten. Security Hub CSPM hilft Ihnen dabei, Ihre Sicherheitstrends zu analysieren und die Sicherheitsprobleme mit der höchsten Priorität in Ihrer AWS Umgebung zu identifizieren.

Informationen zur gemeinsamen Verwendung von Security Hub CSPM GuardDuty und Security Hub finden Sie unter. Integration GuardDuty mit AWS Security Hub CSPM Weitere Informationen zu Security Hub CSPM finden Sie im AWS Security Hub Benutzerhandbuch.

- Amazon Detective — Dieser Service hilft Ihnen dabei, Sicherheitslücken oder verdächtige Aktivitäten zu analysieren, zu untersuchen und schnell die Ursache zu identifizieren. Detective sammelt automatisch Protokolldaten von Ihren AWS Ressourcen. Es verwendet dann Machine Learning, statistische Analysen und die Diagrammtheorie, um Visualisierungen zu erstellen, mit denen Sie effektive Sicherheitsuntersuchungen schneller und effizienter durchführen können. Die vorgefertigten Datenaggregationen, Zusammenfassungen und Kontexte von Detective helfen Ihnen bei der Analyse und Bestimmung der Art und des Ausmaßes potenzieller Sicherheitsprobleme.

  Hinweise zur gemeinsamen Verwendung von GuardDuty und Detective finden Sie unterIntegration GuardDuty mit Amazon Detective. Weitere Informationen zu Detective finden Sie im Amazon Detective User Guide.

- Amazon EventBridge — Dieser Service hilft Ihnen, Benachrichtigungen zu erhalten und nahezu in Echtzeit auf GuardDuty Sicherheitslücken zu reagieren. GuardDuty erzeugt ein Ereignis, wenn sich die Ergebnisse ändern. Sie können wählen, von wie oft Sie die Benachrichtigungen erhalten möchten EventBridge. Weitere Informationen finden Sie unter Was ist Amazon EventBridge im EventBridge Amazon-Benutzerhandbuch.

Compliance mit PCI DSS

GuardDuty unterstützt die Verarbeitung, Speicherung und Übertragung von Kreditkartendaten durch einen Händler oder Dienstleister und wurde als konform mit dem Payment Card Industry (PCI) Data Security Standard (DSS) validiert. Weitere Informationen zu PCI DSS, einschließlich der Möglichkeit, eine Kopie des AWS PCI Compliance Package anzufordern, finden Sie unter PCI DSS Level 1.

Weitere Informationen finden Sie im AWS Sicherheitsblog unter Neuer Drittanbietertest vergleicht Amazon GuardDuty mit Systemen zur Erkennung von Netzwerkeindringlingen.

Preisgestaltung in GuardDuty

Dieser Abschnitt konzentriert sich auf das Kostenloses AWS-Kontingent Modell, das für verschiedene Schutzpläne GuardDuty verwendet wird, und darauf, wie Sie die geschätzten und tatsächlichen

Nutzungskosten einsehen können. Weitere Informationen zu den Preisen aller Schutzpläne in den unterstützten Regionen finden Sie unter GuardDutyPreise.

Kostenloses AWS-Kontingent

Kostenloses AWS-Kontingent hilft Ihnen dabei, die einzelnen Dienste bis zu den angegebenen Limits kostenlos zu erkunden und auszuprobieren AWS-Services . Es gibt drei Kategorien: 12 Monate kostenlose, immer kostenlose und kurzfristige kostenlose Testversionen. Amazon GuardDuty gehört zur Kategorie der kurzfristigen kostenlosen Testversionen und bietet eine kostenlose 30-Tage-Testversion an. Wenn Sie die Nutzung GuardDuty nach Ablauf dieser kostenlosen Testversion fortsetzen, fallen je nachdem, wie Sie diesen Service nutzen, Kosten an.

[1] Ausnahme von der kostenlosen GuardDuty 30-Tage-Testversion

On-demand Malware-Scan (unter Malware Protection for EC2) und Malware Protection for S3 fallen nicht in die Kategorie der kostenlosen GuardDuty 30-Tage-Testversion. Malware Protection for S3 beinhaltet ein kostenloses Kontingent, wohingegen der On-demand Malware-Scan einem nutzungsabhängigen Kostenmodell folgt. Es gibt weder eine kostenlose 30-Tage-Testversion noch ein kostenloses Kontingent mit Malware-Scan. On-demand

Nutzen Sie die kostenlose GuardDuty 30-Tage-Testversion

Wenn Sie es GuardDuty zum ersten Mal in einer verwenden AWS-Region, werden Sie AWS-Konto automatisch für eine kostenlose 30-Tage-Testversion in dieser Region registriert. Einige der Schutzpläne werden ebenfalls automatisch aktiviert und sind in der kostenlosen 30-Tage-Testversion enthalten. Da es GuardDuty sich um einen regionalen Dienst handelt, wird Ihr Konto in dieser Region 30 Tage lang kostenlos getestet, wenn Sie ihn zum ersten Mal GuardDuty in einer anderen Region aktivieren. Wenn Sie mit mehreren Konten in einer GuardDuty Organisation arbeiten, erhält jedes Konto seine eigene kostenlose 30-Tage-Testversion.

Anhand der folgenden Tabelle können Sie überprüfen, welche Schutzpläne standardmäßig aktiviert sind und welche kostenlosen Testversionen verfügbar sind. GuardDuty

Schutzplan	Standardmäßig aktiviert mit GuardDuty	Separate kostenlose Testversion verfügbar [2]	
EKS-Schutz	Ja	Ja	

Schutzplan	Standardmäßig aktiviert mit GuardDuty	Separate kostenlose Testversion verfügbar [2]	
S3-Schutz	Ja	Ja	
Laufzeitüberwachung	Nein	Ja	
Malware-Schutz für EC2 – GuardDuty-initiated Malware-Scan	Ja	Ja	
Malware-Schutz für EC2 – On-demand Malware-Scan in GuardDuty	Nein	Nein [1]	
GuardDuty Malware-Schutz für S3	Nein	Nein [1]	
RDS Protection	Ja	Ja	
Lambda Protection	Ja	Ja	
Malware-Schutz für AWS Backups	Nein	Nein	

[2] GuardDuty Bei der ersten Aktivierung werden die Schutzpläne (außer Runtime Monitoring) automatisch aktiviert und sind in der ersten kostenlosen 30-Tage-Testversion enthalten. Wenn ein vorhandenes GuardDuty Konto nach Ablauf der ersten GuardDuty kostenlosen Testversion einen neuen Schutzplan aktiviert, wird dieser Schutzplan mit einer eigenen kostenlosen 30-Tage-Testversion geliefert. Weitere Informationen zu kostenlosen Testversionen von Schutzplänen finden Sie in dem Dokument, das zu den einzelnen Schutzplänen gehört.

Geschätzte Nutzungskosten während der kostenlosen Testversion anzeigen — Während der kostenlosen 30-Tage-Testversion GuardDuty und möglicherweise eines Schutzplans werden die GuardDuty geschätzten Nutzungskosten für Ihr Konto angezeigt. Wenn Sie ein delegiertes

GuardDuty Administratorkonto haben, können Sie die geschätzten Gesamtkosten für die Nutzung und die Aufschlüsselung auf Kontoebene für alle Mitgliedskonten, die aktiviert wurden, einsehen. GuardDuty Weitere Informationen finden Sie unter Überwachung der GuardDuty Nutzung und Schätzung der Kosten.

Nutzungskosten nach Ablauf der kostenlosen Testphase — Wenn Sie nach Ablauf der kostenlosen Testphase einen der Schutzpläne weiterhin nutzen GuardDuty , fallen für Sie die entsprechenden Nutzungskosten an. Um Ihre Rechnung einzusehen, navigieren Sie in der https://console.aws.amazon.com/costmanagement/Konsole zum Cost Explorer. Weitere Informationen zur AWS Kontoabrechnung finden Sie im AWS Billing Benutzerhandbuch.

Verwenden des Malware-Schutzes für S3 mit kostenlosem Kontingent

Malware Protection for S3 beinhaltet ein kostenloses Kontingent, das mit Ihrem verknüpft ist AWS-Konten. Weitere Informationen finden Sie unter Preise und Nutzungskosten für Malware Protection for S3.

Zugreifen GuardDuty

Amazon GuardDuty ist in den meisten Fällen verfügbar AWS-Regionen. Eine Liste der Regionen, in denen GuardDuty das Produkt derzeit verfügbar ist, finden Sie unterRegionen und Endpunkte.

Sie können es GuardDuty auf eine der folgenden Arten verwenden:

GuardDuty Konsole

https://console.aws.amazon.com/guardduty/

Die Konsole ist eine browserbasierte Schnittstelle für den Zugriff auf und die Verwendung von GuardDuty. Die GuardDuty Konsole bietet Zugriff auf Ihr GuardDuty Konto, Ihre Daten und Ressourcen.

AWS Command Line Interface

Mit AWS Command Line Interface (AWS CLI) können Sie Befehle an der Befehlszeile Ihres Systems ausgeben, um GuardDuty Aufgaben und AWS Aufgaben auszuführen. Die AWS CLI Befehle sind nützlich, wenn Sie Skripts erstellen möchten, die Aufgaben ausführen.

Informationen zur Installation und Verwendung AWS CLI finden Sie im AWS Command Line Interface Benutzerhandbuch. Die verfügbaren AWS CLI Befehle für GuardDuty finden Sie in der AWS CLI Befehlsreferenz.

GuardDuty HTTPS-API

Sie können mithilfe der GuardDuty HTTPS-API AWS programmgesteuert darauf zugreifen GuardDuty , sodass Sie HTTPS-Anfragen direkt an den Dienst senden können. Weitere Informationen finden Sie in der Amazon GuardDuty API-Referenz.

AWS SDKs

AWS bietet Software Development Kits (SDKs), die aus Bibliotheken und Beispielcode für verschiedene Programmiersprachen und Plattformen (Java, Python, Ruby, .NET, iOS, Android und mehr) bestehen. Die SDKs sind gut zur Einrichtung des programmgesteuerten Zugriffs auf GuardDuty geeignet. Weitere Informationen über die AWS -SDKs, das Herunterladen und die Installation finden Sie unter Tools für Amazon Web Services.

Konzepte und Schlüsselbegriffe bei Amazon GuardDuty

Wenn Sie mit Amazon beginnen GuardDuty, können Sie davon profitieren, mehr über die Konzepte und die damit verbundenen Schlüsselbegriffe zu erfahren.

Account

Ein Standardkonto von Amazon Web Services (AWS), das Ihre AWS Ressourcen enthält. Sie können sich AWS mit Ihrem Konto anmelden und es aktivieren GuardDuty.

Sie können auch andere Konten einladen, Ihr AWS Konto zu aktivieren GuardDuty und mit diesem verknüpft zu werden GuardDuty. Wenn Ihre Einladungen akzeptiert werden, wird Ihr Konto als GuardDuty Administratorkonto festgelegt und die hinzugefügten Konten werden zu Ihren Mitgliedskonten. Sie können dann die GuardDuty Ergebnisse dieser Konten in ihrem Namen einsehen und verwalten.

Benutzer des Administratorkontos können die GuardDuty Ergebnisse für ihr eigenes Konto und alle ihre Mitgliedskonten konfigurieren GuardDuty , einsehen und verwalten. Informationen zur Anzahl der Mitgliedskonten, die Ihr Administratorkonto verwalten kann, finden Sie unterGuardDuty Kontingente.

Benutzer von Mitgliedskonten können GuardDuty Ergebnisse in ihrem Konto konfigurieren GuardDuty sowie anzeigen und verwalten (entweder über die GuardDuty Verwaltungskonsole oder die GuardDuty API). Benutzer von Mitgliedskonten können keine Ergebnisse in den Konten anderer Mitglieder anzeigen oder verwalten.

Ein Konto AWS-Konto kann nicht gleichzeitig ein GuardDuty Administratorkonto und ein Mitgliedskonto sein. An AWS-Konto kann nur eine Mitgliedschaftseinladung annehmen. Das Annehmen einer Mitgliedschaftseinladung ist optional.

Weitere Informationen finden Sie unter Mehrere Konten bei Amazon GuardDuty.

Angriffssequenz

Eine Angriffssequenz ist eine Korrelation mehrerer Ereignisse, die, wie von beobachtet GuardDuty, in einer bestimmten Reihenfolge passiert sind, die dem Muster einer verdächtigen Aktivität entspricht. GuardDuty nutzt seine Erweiterte Bedrohungserkennung Fähigkeit, diese mehrstufigen Angriffe zu erkennen, die grundlegende Datenquellen, AWS Ressourcen und Zeitpläne in Ihrem Konto umfassen.

In der folgenden Liste werden die wichtigsten Begriffe im Zusammenhang mit Angriffssequenzen kurz erläutert:

- Indikatoren — Liefert Informationen darüber, warum eine Abfolge von Ereignissen mit einer potenziell verdächtigen Aktivität übereinstimmt.
- Signale — Ein Signal ist eine API-Aktivität, die GuardDuty beobachtet wurde, oder ein bereits entdecktes GuardDuty Ergebnis in Ihrem Konto. Durch die Korrelation der Ereignisse, die in einer bestimmten Reihenfolge in Ihrem Konto beobachtet wurden, wird eine Angriffssequenz GuardDuty identifiziert.

  Es gibt Ereignisse in Ihrem Konto, die nicht auf eine potenzielle Bedrohung hinweisen. GuardDuty betrachtet sie als schwache Signale. Wenn jedoch schwache Signale und GuardDuty Ergebnisse in einer bestimmten Reihenfolge beobachtet werden, die, wenn sie korreliert werden, auf eine potenziell verdächtige Aktivität zurückzuführen sind, GuardDuty führt dies zu einer Feststellung der Angriffssequenz.
- Endpunkte — Informationen über Netzwerkendpunkte, die ein Bedrohungsakteur möglicherweise in einer Angriffssequenz verwendet hat.

Detektor

Amazon GuardDuty ist ein regionaler Service. Wenn Sie eine bestimmte Option aktivieren GuardDuty AWS-Region, AWS-Konto wird Ihnen eine Melder-ID zugewiesen. Diese 32-stellige alphanumerische ID ist einzigartig für Ihr Konto in dieser Region. Wenn Sie beispielsweise GuardDuty für dasselbe Konto in einer anderen Region aktivieren, wird Ihr Konto mit einer anderen Melder-ID verknüpft. Das Format einer Detektor-ID ist `12abc34d567e8fa901bc2d34e56789f0`.

Alle GuardDuty Ergebnisse, Konten und Aktionen zur Verwaltung von Ergebnissen und zum GuardDuty Service verwenden die Detektor-ID, um einen API-Vorgang auszuführen.

Um die `detectorId` für Ihr Konto und Ihre aktuelle Region geltenden Daten zu finden, gehen Sie in der https://console.aws.amazon.com/guardduty/Konsole auf die Seite „Einstellungen“ oder führen Sie die ListDetectorsAPI aus.

> **Note**
>
> In Umgebungen mit mehreren Konten werden alle Erkenntnisse für Mitgliedskonten zum Detektor des Administratorkontos weitergeleitet.

Einige GuardDuty Funktionen werden über den Detektor konfiguriert, z. B. die Konfiguration der Häufigkeit von Benachrichtigungen über CloudWatch Ereignisse und die Aktivierung oder Deaktivierung optionaler Schutzpläne für GuardDuty die Verarbeitung.

Verwenden Sie den Malware-Schutz für S3 innerhalb GuardDuty

Wenn Sie Malware Protection for S3 in einem Konto aktivieren, auf dem diese Option aktiviert GuardDuty ist, werden die Aktionen von Malware Protection for S3 wie das Aktivieren, Bearbeiten und Deaktivieren einer geschützten Ressource nicht mit der Detektor-ID verknüpft.

Wenn Sie die Bedrohungserkennungsoption Malware Protection for S3 nicht aktivieren GuardDuty und auswählen, wird keine Detektor-ID für Ihr Konto erstellt.

Grundlegende Datenquellen

Der Ursprung oder Speicherort eines Datensatzes. Um eine nicht autorisierte oder unerwartete Aktivität in Ihrer AWS Umgebung zu erkennen. GuardDuty analysiert und verarbeitet Daten aus AWS CloudTrail Ereignisprotokollen, AWS CloudTrail Verwaltungsereignissen, AWS CloudTrail Datenereignissen für S3, VPC-Flussprotokollen und DNS-Protokollen, siehe GuardDuty grundlegende Datenquellen.

Merkmal

Ein für Ihren GuardDuty Schutzplan konfiguriertes Feature-Objekt hilft dabei, unbefugte oder unerwartete Aktivitäten in Ihrer AWS Umgebung zu erkennen. Jeder GuardDuty Schutzplan konfiguriert das entsprechende Featureobjekt für die Analyse und Verarbeitung von Daten. Zu den Featureobjekten gehören EKS-Auditprotokolle, Überwachung der RDS-Anmeldeaktivität, Lambda-Netzwerkaktivitätsprotokolle und EBS-Volumes. Weitere Informationen finden Sie unter Funktionsnamen für Schutzpläne in der GuardDuty API.

Erkenntnis

Ein von GuardDuty erkanntes potenzielles Sicherheitsrisiko. Weitere Informationen finden Sie unter GuardDuty Amazon-Ergebnisse verstehen und generieren.

Die Ergebnisse werden in der GuardDuty Konsole angezeigt und enthalten eine detaillierte Beschreibung des Sicherheitsproblems. Sie können Ihre generierten Ergebnisse auch abrufen, indem Sie die Operationen GetFindingsund die ListFindingsAPI aufrufen.

Sie können Ihre GuardDuty Ergebnisse auch über Amazon CloudWatch Events einsehen. GuardDuty sendet Ergebnisse CloudWatch über das HTTPS-Protokoll an Amazon. Weitere Informationen finden Sie unter Bearbeitung von GuardDuty Ergebnissen mit Amazon EventBridge.

IAM role (IAM-Rolle)

Dies ist die IAM-Rolle mit den erforderlichen Berechtigungen zum Scannen des S3-Objekts. Wenn das Taggen gescannter Objekte aktiviert ist, helfen die PassRole IAM-Berechtigungen dabei, dem gescannten Objekt Tags GuardDuty hinzuzufügen.

Ressource für den Malware-Schutzplan

Nachdem Sie den Malware-Schutz für S3 für einen Bucket aktiviert haben, GuardDuty wird eine Ressource für den Malware-Schutzplan erstellt. Diese Ressource ist mit der Malware Protection-Plan-ID verknüpft, einer eindeutigen Kennung für Ihren geschützten Bucket. Verwenden Sie die Ressource des Malware-Schutzplans, um API-Operationen auf einer geschützten Ressource durchzuführen.

Geschützter Bucket (geschützte Ressource)

Ein Amazon S3 S3-Bucket gilt als geschützt, wenn Sie Malware Protection for S3 für diesen Bucket aktivieren und sein Schutzstatus auf Aktiv geändert wird.

GuardDuty unterstützt nur einen S3-Bucket als geschützte Ressource.

Schutzstatus

Der Status, der mit der Ressource Ihres Malware-Schutzplans verknüpft ist. Nachdem Sie Malware Protection for S3 für Ihren Bucket aktiviert haben, gibt dieser Status an, ob Ihr Bucket korrekt eingerichtet ist oder nicht.

S3-Objektpräfix

In einem Amazon Simple Storage Service (Amazon S3) -Bucket können Sie Präfixe verwenden, um Ihren Speicher zu organisieren. Ein Präfix ist eine logische Gruppierung der Objekte in einem S3-Bucket. Weitere Informationen finden Sie unter Objekte organisieren und auflisten im Amazon S3 S3-Benutzerhandbuch.

Scan-Optionen

Wenn GuardDuty Malware Protection for EC2 aktiviert ist, können Sie angeben, welche Amazon EC2-Instances und Amazon Elastic Block Store (EBS) -Volumes gescannt oder übersprungen werden sollen. Mit diesem Feature können Sie die vorhandenen Tags, die Ihren EC2-Instances und Ihrem EBS-Volume zugeordnet sind, entweder zu einer Liste mit Einschluss-Tags oder einer Liste mit Ausschluss-Tags hinzufügen. Die Ressourcen, die mit den Tags verknüpft sind, die Sie zu einer Liste mit Einschlusstags hinzufügen, werden auf Malware gescannt, und die Ressourcen, die zu einer Ausschlusstag-Liste hinzugefügt wurden, werden nicht gescannt. Weitere Informationen finden Sie unter Scan-Optionen mit benutzerdefinierten Tags.

Aufbewahrung von Snapshots

Wenn GuardDuty Malware Protection for EC2 aktiviert ist, besteht die Möglichkeit, die Snapshots Ihrer EBS-Volumes in Ihrem Konto aufzubewahren. AWS GuardDuty generiert die Replikat-EBS-Volumes auf der Grundlage der Snapshots Ihrer EBS-Volumes. Sie können die Snapshots Ihrer EBS-Volumes nur dann beibehalten, wenn der Malware Protection for EC2-Scan Malware in den EBS-Replikat-Volumes erkennt. Wenn auf den EBS-Replikat-Volumes keine Malware erkannt wird, werden die Snapshots Ihrer EBS-Volumes unabhängig von der Aufbewahrungseinstellung für Snapshots GuardDuty automatisch gelöscht. Weitere Informationen finden Sie unter Snapshot-Beibehaltung.

Regel zur Unterdrückung

Unterdrückungsregeln ermöglichen die Einrichtung sehr spezifischer Kombinationen von Attributen, um Ergebnisse zu unterdrücken. Sie können beispielsweise über den GuardDuty Filter eine Regel definieren, um nur die Instances in einer bestimmten VPC, auf der ein bestimmtes AMI oder mit einem bestimmten EC2-Tag ausgeführt wird, automatisch zu archivieren`Recon:EC2/Portscan`. Diese Regel würde dazu führen, dass Port-Scan-Ergebnisse von den Instances automatisch archiviert werden, die die Kriterien erfüllen. Es ermöglicht jedoch weiterhin Warnmeldungen, wenn Instances GuardDuty entdeckt werden, die andere bösartige Aktivitäten wie das Mining von Kryptowährungen ausführen.

Die im GuardDuty Administratorkonto definierten Unterdrückungsregeln gelten für die Mitgliedskonten GuardDuty . GuardDuty Mitgliedskonten können die Unterdrückungsregeln nicht ändern.

Bei Unterdrückungsregeln werden GuardDuty trotzdem alle Ergebnisse generiert. Die Unterdrückungsregeln sorgen für eine Unterdrückung von Ergebnissen, während gleichzeitig ein vollständiger und unveränderlicher Verlauf aller Aktivitäten aufgezeichnet wird.

Gewöhnlich werden Unterdrückungsregeln verwendet, um Ergebnisse zu verbergen, die Sie als falsch positive Ergebnisse für Ihre Umgebung ermittelt haben, und um das Rauschen durch Ergebnisse mit niedrigem Wert zu reduzieren, sodass Sie sich auf größere Bedrohungen konzentrieren können. Weitere Informationen finden Sie unter Unterdrückungsregeln in GuardDuty.

Liste vertrauenswürdiger IPs

Eine Liste vertrauenswürdiger IP-Adressen für die hochsichere Kommunikation mit Ihrer AWS Umgebung. GuardDuty generiert keine Ergebnisse auf der Grundlage vertrauenswürdiger

IP-Listen. Weitere Informationen finden Sie unter Anpassen der Bedrohungserkennung mit Entitätenlisten und IP-Adresslisten.

Liste der bedrohlichen IP-Adressen

Eine Liste bekannter böswilliger IP-Adressen. Generiert nicht nur Ergebnisse aufgrund einer potenziell verdächtigen Aktivität, GuardDuty sondern generiert auch Ergebnisse auf der Grundlage dieser Bedrohungslisten. Weitere Informationen finden Sie unter Anpassen der Bedrohungserkennung mit Entitätenlisten und IP-Adresslisten.

Erste Schritte mit GuardDuty

Dieses Tutorial bietet eine praktische Einführung in. GuardDuty Die Mindestanforderungen für die Aktivierung GuardDuty als eigenständiges Konto oder als GuardDuty Administrator mit AWS Organizations werden in Schritt 1 behandelt. Die Schritte 2 bis 5 behandeln die Verwendung zusätzlicher Funktionen, die von empfohlen werden GuardDuty , um das Beste aus Ihren Ergebnissen herauszuholen.

Themen

- Bevor Sie beginnen
- Schritt 1: Amazon aktivieren GuardDuty
- Schritt 2: Beispiel-Erkenntnisse generieren und die grundlegenden Abläufe erkunden
- Schritt 3: Konfigurieren Sie den Export von GuardDuty Ergebnissen in einen Amazon S3 S3-Bucket
- Schritt 4: Richten Sie die GuardDuty Suche nach Benachrichtigungen über SNS ein
- Nächste Schritte

Bevor Sie beginnen

GuardDuty ist ein Dienst zur Bedrohungserkennung, Grundlegende Datenquellen der AWS CloudTrail Verwaltungsereignisse, Amazon VPC Flow Logs und Amazon Route 53 Resolver DNS-Abfrageprotokolle überwacht. GuardDutyanalysiert auch Funktionen, die mit seinen Schutztypen verknüpft sind, nur wenn Sie sie separat aktivieren. Zu den Funktionen gehören Kubernetes-Auditprotokolle, RDS-Anmeldeaktivitäten, AWS CloudTrail Datenereignisse für Amazon S3, Amazon EBS-Volumes, Runtime Monitoring und Lambda-Netzwerkaktivitätsprotokolle. Durch die Verwendung dieser Datenquellen und Funktionen (sofern aktiviert) werden Sicherheitslücken für GuardDuty Ihr Konto generiert.

Nach der Aktivierung beginnt es GuardDuty, Ihr Konto auf der Grundlage der Aktivitäten in grundlegenden Datenquellen auf potenzielle Bedrohungen zu überwachen. Standardmäßig Erweiterte Bedrohungserkennung ist es für alle aktiviert, AWS-Konten die es aktiviert GuardDuty haben. Diese Funktion erkennt mehrstufige Angriffssequenzen, die sich über mehrere grundlegende Datenquellen, AWS Ressourcen und Zeiträume in Ihrem Konto erstrecken. Um potenzielle Bedrohungen für bestimmte AWS Ressourcen zu erkennen, können Sie sich dafür entscheiden, anwendungsfallorientierte Schutzpläne zu aktivieren, die Folgendes bieten: GuardDuty Weitere Informationen finden Sie unter Eigenschaften von GuardDuty.

Sie müssen keine der grundlegenden Datenquellen explizit aktivieren. Wenn Sie S3 Protection aktivieren, müssen Sie die Amazon S3 S3-Datenereignisprotokollierung nicht explizit aktivieren. Ebenso müssen Sie bei der Aktivierung von EKS Protection die Amazon EKS-Audit-Logs nicht explizit aktivieren. Amazon GuardDuty bezieht unabhängige Datenströme direkt von diesen Diensten.

Für ein neues GuardDuty Konto sind einige der verfügbaren Schutzarten, die in einem unterstützt werden, AWS-Region standardmäßig aktiviert und in der 30-tägigen kostenlosen Testphase enthalten. Sie können einen oder alle von ihnen deaktivieren. Wenn Sie bereits AWS-Konto mit GuardDuty aktiviert sind, können Sie wählen, ob Sie einige oder alle Schutzpläne aktivieren möchten, die in Ihrer Region verfügbar sind. Eine Übersicht über die Schutzpläne und darüber, welche Schutzpläne standardmäßig aktiviert werden, finden Sie unterPreisgestaltung in GuardDuty.

Beachten Sie bei der Aktivierung GuardDuty die folgenden Punkte:

- GuardDuty ist ein regionaler Dienst, was bedeutet, dass alle Konfigurationsverfahren, die Sie auf dieser Seite ausführen, in jeder Region, mit der Sie überwachen möchten, wiederholt werden müssen GuardDuty.

  Wir empfehlen dringend, die Aktivierung GuardDuty in allen unterstützten AWS Regionen durchzuführen. Auf diese Weise können GuardDuty auch in Regionen, die Sie nicht aktiv nutzen, Erkenntnisse über unbefugte oder ungewöhnliche Aktivitäten generiert werden. Dies ermöglicht auch GuardDuty die Überwachung von AWS CloudTrail Ereignissen für globale AWS Dienste wie IAM. Wenn diese Option nicht in allen unterstützten Regionen aktiviert GuardDuty ist, ist ihre Fähigkeit zur Erkennung von Aktivitäten, die globale Dienste betreffen, eingeschränkt. Eine vollständige Liste der Regionen, in denen GuardDuty es verfügbar ist, finden Sie unterRegionen und Endpunkte.
- Jeder Benutzer mit Administratorrechten in einem AWS Konto kann diese Option aktivieren GuardDuty. Gemäß der bewährten Sicherheitsmethode der geringsten Rechte wird jedoch empfohlen, eine IAM-Rolle, einen Benutzer oder eine Gruppe zu erstellen, die GuardDuty speziell verwaltet werden soll. Informationen zu den für die Aktivierung erforderlichen Berechtigungen GuardDuty finden Sie unterFür die Aktivierung sind Berechtigungen erforderlich GuardDuty.
- Wenn Sie es GuardDuty zum ersten Mal in einer beliebigen AWS-Region Region aktivieren, werden standardmäßig auch alle verfügbaren Schutztypen aktiviert, die in dieser Region unterstützt werden, einschließlich Malware Protection for EC2. GuardDuty erstellt eine dienstverknüpfte Rolle für Ihr Konto namens. `AWSServiceRoleForAmazonGuardDuty` Diese Rolle umfasst die Berechtigungen und Vertrauensrichtlinien, die es ermöglichen, Ereignisse direkt aus GuardDuty dem zu verarbeiten und zu analysieren, GuardDuty grundlegende Datenquellen um daraus Sicherheitsresultate zu generieren. Malware

Protection for EC2 erstellt eine weitere dienstbezogene Rolle für Ihr Konto mit dem Namen. `AWSServiceRoleForAmazonGuardDutyMalwareProtection` Diese Rolle umfasst die Berechtigungen und Vertrauensrichtlinien, die es Malware Protection for EC2 ermöglichen, Scans ohne Agenten durchzuführen, um Malware in Ihrem Konto zu erkennen. GuardDuty Sie ermöglicht es GuardDuty , einen EBS-Volume-Snapshot in Ihrem Konto zu erstellen und diesen Snapshot mit dem GuardDuty Dienstkonto zu teilen. Weitere Informationen finden Sie unter Service-linked Rollenberechtigungen für GuardDuty. Weitere Informationen zu serviceverknüpften Rollen finden Sie unter Verwenden serviceverknüpfter Rollen.

- Wenn Sie Ihr Konto GuardDuty zum ersten Mal in einer Region aktivieren, wird Ihr AWS Konto automatisch für eine GuardDuty kostenlose 30-Tage-Testversion für diese Region registriert.

Im folgenden Video wird erklärt, wie Sie mit einem Administratorkonto beginnen GuardDuty und es für mehrere Mitgliedskonten aktivieren können.

Erste Schritte: Amazon GuardDuty für eigenständige Umgebungen oder Umgebungen mit mehreren Konten aktivieren

Schritt 1: Amazon aktivieren GuardDuty

Der erste Schritt zur Verwendung GuardDuty besteht darin, es in Ihrem Konto zu aktivieren. Nach der Aktivierung GuardDuty wird sofort mit der Überwachung auf Sicherheitsbedrohungen in der aktuellen Region begonnen.

Wenn Sie die GuardDuty Ergebnisse für andere Konten innerhalb Ihrer Organisation als GuardDuty Administrator verwalten möchten, müssen Sie Mitgliedskonten hinzufügen und diese ebenfalls aktivieren GuardDuty .

> **Note**
>
> Wenn Sie den GuardDuty Malware-Schutz für S3 ohne Aktivierung aktivieren möchten GuardDuty, finden Sie die entsprechenden Schritte unterGuardDuty Malware-Schutz für S3.

Standalone account environment

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/
2. Wählen Sie die Option Amazon GuardDuty — Alle Funktionen.
3. Wählen Sie Erste Schritte.
4. Sehen Sie sich auf der GuardDuty Seite Willkommen bei die Servicebedingungen an. Wählen Sie Enable (Aktivieren) GuardDuty aus.

Multi-account environment

> **Important**
>
> Voraussetzung für diesen Vorgang ist, dass Sie derselben Organisation angehören wie alle Konten, die Sie verwalten möchten, und Zugriff auf das AWS Organizations Verwaltungskonto haben müssen, um einen Administrator GuardDuty innerhalb Ihrer Organisation delegieren zu können. Für die Delegierung eines Administrators sind möglicherweise zusätzliche Berechtigungen erforderlich. Weitere Informationen finden Sie unter Für die Benennung eines delegierten GuardDuty Administratorkontos sind Berechtigungen erforderlich.

Um ein GuardDuty delegiertes Administratorkonto zu bestimmen

1. Öffnen Sie die AWS Organizations Konsole unter https://console.aws.amazon.com/organizations/und verwenden Sie das Verwaltungskonto.
2. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Ist in Ihrem Konto GuardDuty bereits aktiviert?

   - Falls GuardDuty es noch nicht aktiviert ist, können Sie Erste Schritte auswählen und dann auf der Seite Willkommen GuardDuty bei einen GuardDuty delegierten Administrator benennen.
   - Wenn diese Option aktiviert GuardDuty ist, können Sie auf der Seite Einstellungen einen GuardDuty delegierten Administrator benennen.
3. Geben Sie die zwölfstellige AWS Konto-ID des Kontos ein, das Sie als delegierten Administrator für die Organisation festlegen möchten, und wählen Sie GuardDuty Delegieren aus.

   > **Note**
   >
   > Falls dies noch nicht aktiviert GuardDuty ist, wird durch die Benennung eines delegierten Administrators die Aktivierung GuardDuty für dieses Konto in Ihrer aktuellen Region aktiviert.

So fügen Sie Mitgliedskonten hinzu

Dieses Verfahren umfasst das Hinzufügen von Mitgliederkonten zu einem GuardDuty delegierten Administratorkonto durch. AWS Organizations Es besteht auch die Möglichkeit, Mitglieder auf Einladung hinzuzufügen. Weitere Informationen zu beiden Methoden zum Zuordnen von Mitgliedern finden Sie GuardDuty unter. Mehrere Konten bei Amazon GuardDuty

1. Melden Sie sich im delegierten Administratorkonto an
2. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/
3. Wählen Sie im Navigationsbereich Settings (Einstellungen) und dann Accounts (Konten) aus.

   In der Kontentabelle werden alle Konten in der Organisation angezeigt.
4. Wählen Sie die Konten aus, die Sie als Mitglieder hinzufügen möchten, indem Sie das Kontrollkästchen neben der Konto-ID aktivieren. Wählen Sie dann im Menü Aktion die Option Mitglied hinzufügen.

> **Tip**
>
> Sie können das Hinzufügen neuer Konten als Mitglieder automatisieren, indem Sie die Auto-enableFunktion aktivieren. Dies gilt jedoch nur für Konten, die Ihrer Organisation beitreten, nachdem die Funktion aktiviert wurde.

Schritt 2: Beispiel-Erkenntnisse generieren und die grundlegenden Abläufe erkunden

Wenn ein Sicherheitsproblem GuardDuty entdeckt wird, wird ein Befund generiert. Ein GuardDuty Befund ist ein Datensatz, der Details zu diesem speziellen Sicherheitsproblem enthält. Die Einzelheiten der Erkenntnis können Ihnen bei der Untersuchung des Problems helfen.

GuardDuty unterstützt die Generierung von Stichprobenergebnissen mit Platzhalterwerten, anhand derer Sie die GuardDuty Funktionalität testen und sich mit den Ergebnissen vertraut machen können, bevor Sie auf ein echtes Sicherheitsproblem reagieren müssen, das von entdeckt wurde. GuardDuty Folgen Sie der nachstehenden Anleitung, um Beispielergebnisse für jeden Befundtyp zu generieren GuardDuty, der unter verfügbar ist. Weitere Möglichkeiten zur Generierung von Stichprobenergebnissen, einschließlich der Generierung eines simulierten Sicherheitsereignisses in Ihrem Konto, finden Sie unter. Beispielerkenntnisse

So erstellen und untersuchen Sie Beispiel-Erkenntnisse

1. Wählen Sie im Navigationsbereich Settings (Einstellungen).
2. Klicken Sie auf der Seite Settings unter Sample findings auf Generate sample findings.
3. Wählen Sie im Navigationsbereich Zusammenfassung aus, um die in Ihrer AWS Umgebung generierten Erkenntnisse zu den Ergebnissen anzuzeigen. Weitere Informationen zu den Komponenten des Übersichts-Dashboards finden Sie unter Übersichts-Dashboard in Amazon GuardDuty.
4. Wählen Sie im Navigationsbereich Findings aus. Die Beispiel-Erkenntnisse werden auf der Seite Aktuelle Erkenntnisse mit dem Präfix [SAMPLE] angezeigt.
5. Wählen Sie eine Erkenntnis aus der Liste aus, um Details zur Erkenntnis anzuzeigen.

    - Sie können die verschiedenen Informationsfelder überprüfen, die im Bereich mit den Erkenntnisdetails verfügbar sind. Verschiedene Arten von Erkenntnissen können

unterschiedliche Felder haben. Weitere Informationen zu den verfügbaren Feldern für alle Erkenntnistypen finden Sie unter Erkenntnisdetails. In der Detailansicht können Sie die folgenden Aktionen durchführen:

- Wählen Sie oben im Bereich die Erkenntnis-ID aus, um die vollständigen JSON-Details für die Erkenntnis zu öffnen. Die vollständige JSON-Datei kann auch von dieser Ansicht heruntergeladen werden. Das JSON enthält einige zusätzliche Informationen, die nicht in der Konsolenansicht enthalten sind. Es ist das Format, das von anderen Tools und Services aufgenommen werden kann.
- Sehen Sie sich den Abschnitt Betroffene Ressource an. Bei einem echten Ergebnis helfen Ihnen die Informationen hier dabei, eine Ressource in Ihrem Konto zu identifizieren, die untersucht werden sollte, und sie enthalten Links zu den entsprechenden AWS-Managementkonsole Ressourcen, die umsetzbar sind.
- Wählen Sie das + oder - beim Lupensymbol, um einen inklusiven oder exklusiven Filter für dieses Detail zu erstellen. Weitere Informationen zu Filtern finden Sie unter Ergebnisse filtern in GuardDuty.

6. Archivieren Sie all Ihre Beispiel-Erkenntnisse

   a. Wählen Sie alle Erkenntnisse aus, indem Sie das Kontrollkästchen oben in der Liste aktivieren.

   b. Deaktivieren Sie alle Erkenntnisse, die Sie behalten möchten.

   c. Wählen Sie das Menü Aktionen und dann Archivieren, um die Beispiel-Erkenntnisse auszublenden.

> **Note**
>
> Um die archivierten Erkenntnisse anzuzeigen, wählen Sie Aktuell und dann Archiviert, um zur Erkenntnisansicht zu wechseln.

Schritt 3: Konfigurieren Sie den Export von GuardDuty Ergebnissen in einen Amazon S3 S3-Bucket

GuardDuty empfiehlt, Einstellungen für den Export von Ergebnissen zu konfigurieren, da Sie so Ihre Ergebnisse in einen S3-Bucket exportieren können, um sie nach Ablauf der Aufbewahrungsfrist von GuardDuty 90 Tagen auf unbestimmte Zeit zu speichern. Auf diese Weise können Sie

Aufzeichnungen über die Ergebnisse führen oder Probleme in Ihrer AWS Umgebung im Laufe der Zeit verfolgen. GuardDuty verschlüsselt die Ergebnisdaten in Ihrem S3-Bucket mithilfe von AWS Key Management Service (AWS KMS key). Um die Einstellungen zu konfigurieren, müssen Sie GuardDuty der Berechtigung einen KMS-Schlüssel geben. Ausführlichere Schritte finden Sie unterGenerierte Ergebnisse nach Amazon S3 exportieren.

Um GuardDuty Ergebnisse in einen Amazon S3 S3-Bucket zu exportieren

1. Richtlinie an KMS-Schlüssel anhängen

   a. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Konsole AWS Key Management Service (AWS KMS) unter https://console.aws.amazon.com/kms.

   b. Um das zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.

   c. Klicken Sie im Navigationsbereich auf Kundenverwaltete Schlüssel.

   d. Wählen Sie einen vorhandenen KMS-Schlüssel aus, oder führen Sie die Schritte zum Erstellen eines KMS-Schlüssels mit symmetrischer Verschlüsselung im Entwicklerhandbuch aus.AWS Key Management Service

      Die Region Ihres KMS-Schlüssels und Ihres Amazon S3 S3-Buckets müssen identisch sein.

      Kopieren Sie den Schlüssel ARN auf einen Notizblock, um ihn in den späteren Schritten zu verwenden.

   e. Wählen Sie im Abschnitt Schlüsselrichtlinie Ihres KMS-Schlüssels die Option Bearbeiten aus. Wenn Zur Richtlinienansicht wechseln angezeigt wird, wählen Sie diese aus, um die Schlüsselrichtlinie anzuzeigen, und klicken Sie dann auf Bearbeiten.

   f. Kopieren Sie den folgenden Richtlinienblock in Ihre KMS-Schlüsselrichtlinie:

```
{
    "Sid": "AllowGuardDutyKey",
    "Effect": "Allow",
    "Principal": {
        "Service": "guardduty.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey",
    "Resource": "KMS key ARN",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "123456789012",
```

```
            "aws:SourceArn":
 "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
        }
    }
}
```

Bearbeiten Sie die Richtlinie, indem Sie die folgenden Werte ersetzen, die *red*im Richtlinienbeispiel formatiert sind:

1. *KMS key ARN*Ersetzen Sie durch den Amazon-Ressourcennamen (ARN) des KMS-Schlüssels. Informationen zur Suche nach dem Schlüssel-ARN finden Sie unter Suchen der Schlüssel-ID und des ARN im AWS Key Management Service Entwicklerhandbuch.
2. *123456789012*Ersetzen Sie es durch die AWS-Konto ID, der das GuardDuty Konto gehört, das die Ergebnisse exportiert.
3. *Region2*Ersetzen Sie durch den AWS-Region Ort, an dem die GuardDuty Ergebnisse generiert wurden.
4. *SourceDetectorID*Ersetzen Sie es durch das GuardDuty Konto in der spezifischen Region, in der die Ergebnisse generiert wurden. `detectorID`

   Das `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

2. Richtlinie an Amazon S3 S3-Bucket anhängen

   Wenn Sie noch keinen Amazon S3 S3-Bucket haben, in den Sie diese Ergebnisse exportieren möchten, finden Sie weitere Informationen unter Erstellen eines Buckets im Amazon S3 S3-Benutzerhandbuch.

   a. Führen Sie die Schritte unter So erstellen oder bearbeiten Sie eine Bucket-Richtlinie im Amazon S3 S3-Benutzerhandbuch aus, bis die Seite Bucket-Richtlinie bearbeiten angezeigt wird.

   b. Die Beispielrichtlinie zeigt, wie Sie die GuardDuty Erlaubnis zum Exportieren von Ergebnissen in Ihren Amazon S3 S3-Bucket erteilen. Wenn Sie den Pfad ändern, nachdem Sie Exportergebnisse konfiguriert haben, müssen Sie die Richtlinie ändern, um die Erlaubnis für den neuen Speicherort zu erteilen.

      Kopieren Sie die folgende Beispielrichtlinie und fügen Sie sie in den Bucket-Richtlinieneditor ein.

Wenn Sie die Richtlinienerklärung vor der endgültigen Aussage hinzugefügt haben, fügen Sie vor dem Hinzufügen dieser Aussage ein Komma hinzu. Stellen Sie sicher, dass die JSON-Syntax Ihrer KMS-Schlüsselrichtlinie gültig ist.

Beispiel für eine S3-Bucket-Richtlinie

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Allow GetBucketLocation",
            "Effect": "Allow",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:GetBucketLocation",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "aws:SourceArn": "arn:aws:guardduty:us-
east-2:123456789012:detector/SourceDetectorID"

                }
            }
        },
        {
            "Sid": "Allow PutObject",
            "Effect": "Allow",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional
 prefix]/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
```

```
                    "aws:SourceArn": "arn:aws:guardduty:us-
east-2:123456789012:detector/SourceDetectorID"

                }
            }
        },
        {
            "Sid": "Deny unencrypted object uploads",
            "Effect": "Deny",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional
 prefix]/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption": "aws:kms"
                }
            }
        },
        {
            "Sid": "Deny incorrect encryption header",
            "Effect": "Deny",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional
 prefix]/*",
            "Condition": {
                "StringNotEquals": {
                "s3:x-amz-server-side-encryption-aws-kms-key-id":
 "arn:aws:kms:us-east-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
                }
            }
        },
        {
            "Sid": "Deny non-HTTPS access",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
```

```
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional
 prefix]/*",
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

c. Bearbeiten Sie die Richtlinie, indem Sie die folgenden Werte ersetzen, die *red*im Richtlinienbeispiel formatiert sind:

1. *Amazon S3 bucket ARN*Ersetzen Sie es durch den Amazon-Ressourcennamen (ARN) des Amazon S3-Buckets. Sie finden den Bucket-ARN auf der Seite Bucket-Richtlinie bearbeiten in der https://console.aws.amazon.com/s3/Konsole.
2. *123456789012*Ersetzen Sie ihn durch die AWS-Konto ID, der das GuardDuty Konto gehört, das die Ergebnisse exportiert.
3. *Region2*Ersetzen Sie durch den AWS-Region Ort, an dem die GuardDuty Ergebnisse generiert wurden.
4. *SourceDetectorID*Ersetzen Sie es durch das GuardDuty Konto in der spezifischen Region, in der die Ergebnisse generiert wurden. `detectorID`

   Das `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.
5. Ersetzen Sie einen *[optional prefix]* Teil des *S3 bucket ARN/[optional prefix]* Platzhalterwerts durch einen optionalen Ordnerspeicherort, in den Sie die Ergebnisse exportieren möchten. Weitere Informationen zur Verwendung von Präfixen finden Sie unter Objekte mithilfe von Präfixen organisieren im Amazon S3 S3-Benutzerhandbuch.

   Wenn Sie einen optionalen Ordnerspeicherort angeben, der noch nicht existiert, GuardDuty wird dieser Speicherort nur erstellt, wenn das mit dem S3-Bucket verknüpfte Konto mit dem Konto identisch ist, das die Ergebnisse exportiert. Wenn Sie Ergebnisse in einen S3-Bucket exportieren, der zu einem anderen Konto gehört, muss der Speicherort des Ordners bereits vorhanden sein.

6. *KMS key ARN*Ersetzen Sie ihn durch den Amazon-Ressourcennamen (ARN) des KMS-Schlüssels, der mit der Verschlüsselung der in den S3-Bucket exportierten Ergebnisse verknüpft ist. Informationen zur Suche nach dem Schlüssel-ARN finden Sie unter Suchen der Schlüssel-ID und des ARN im AWS Key Management Service Entwicklerhandbuch.

3. Schritte in der GuardDuty Konsole

   a. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   b. Wählen Sie im Navigationsbereich Settings (Einstellungen).

   c. Wählen Sie auf der Seite Einstellungen unter Exportoptionen für Ergebnisse für den S3-Bucket die Option Jetzt konfigurieren (oder je nach Bedarf Bearbeiten) aus.

   d. Geben Sie für den S3-Bucket ARN **`bucket ARN`** den ein, an den Sie die Ergebnisse senden möchten. Informationen zum Anzeigen des Bucket-ARN finden Sie unter Eigenschaften für einen S3-Bucket anzeigen im Amazon S3 S3-Benutzerhandbuch.

   e. Geben Sie für KMS-Schlüssel-ARN den ein**`key ARN`**. Informationen zum Auffinden des Schlüssel-ARN finden Sie unter Suchen der Schlüssel-ID und des Schlüssel-ARN im AWS Key Management Service Entwicklerhandbuch.

   f. Wählen Sie Speichern.

Schritt 4: Richten Sie die GuardDuty Suche nach Benachrichtigungen über SNS ein

GuardDuty integriert sich in Amazon EventBridge, wodurch Ergebnisdaten zur Verarbeitung an andere Anwendungen und Dienste gesendet werden können. Mit EventBridge Hilfe von GuardDuty Ergebnissen können Sie automatische Antworten auf Ihre Ergebnisse einleiten, indem Sie Findereignisse mit Zielen wie AWS Lambda Funktionen, Amazon EC2 Systems Manager Manager-Automatisierung, Amazon Simple Notification Service (SNS) und mehr verknüpfen.

In diesem Beispiel erstellen Sie ein SNS-Thema, das das Ziel einer EventBridge Regel sein soll. Anschließend erstellen Sie EventBridge eine Regel, die Ergebnisdaten erfasst. GuardDuty Die resultierende Regel leitet die Erkenntnisdetails an eine E-Mail-Adresse weiter. Weitere Informationen dazu, wie Sie Erkenntnisse an Slack oder Amazon Chime senden und auch die Arten der Benachrichtigungen zu Erkenntnissen ändern können, finden Sie unter Ein Amazon SNS SNS-Thema und einen Endpunkt einrichten.

So erstellen Sie ein SNS-Thema für Ihre Benachrichtigungen zu Erkenntnissen

1. Öffnen Sie die Amazon-SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Wählen Sie im Navigationsbereich Themen aus.
3. Wählen Sie Create Topic (Thema erstellen) aus.
4. Wählen Sie für Typ die Option Standard.
5. Geben Sie unter Name **`GuardDuty`** ein.
6. Wählen Sie Create Topic (Thema erstellen) aus. Die Themendetails für Ihr neues Thema werden geöffnet.
7. Wählen Sie im Abschnitt Subscriptions (Abonnements) die Option Create subscription (Abonnement erstellen) aus.
8. Wählen Sie unter Protocol (Protokoll) die Option Email (E-Mail) aus.
9. Geben Sie als Endpunkt die E-Mail-Adresse ein, an die Benachrichtigungen gesendet werden sollen.
10. Wählen Sie Create subscription (Abonnement erstellen) aus.

    Sie müssen Ihre E-Mail-Adresse bestätigen, nachdem Sie das Abonnement erstellt haben.
11. Um nach einer Abonnementnachricht zu suchen, gehen Sie zu Ihrem E-Mail-Posteingang und wählen Sie in der Abonnementnachricht die Option Abonnement bestätigen.

> **Note**
>
> Um den Status der E-Mail-Bestätigung zu überprüfen, rufen Sie die SNS-Konsole auf und wählen Sie Abonnements.

Um eine EventBridge Regel zu erstellen, um GuardDuty Ergebnisse zu erfassen und zu formatieren

1. Öffnen Sie die EventBridge Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie im Navigationsbereich Regeln aus.
3. Wählen Sie Regel erstellen aus.
4. Geben Sie einen Namen und eine Beschreibung für die Regel ein.

   Eine Regel darf nicht denselben Namen wie eine andere Regel in derselben Region und auf demselben Event Bus haben.
5. Bei Event bus (Ereignisbus) wählen Sie default (Standard) aus.

6. Bei Regeltyp wählen Sie Regel mit einem Ereignismuster aus.
7. Wählen Sie Weiter aus.
8. Wählen Sie unter Event source (Ereignisquelle) AWS events (Ereignisse) aus.
9. Wählen Sie für Ereignismuster die Option Ereignismusterformular.
10. Als Event source (Ereignisquelle) wählen Sie AWS -Services aus.
11. Wählen Sie unter AWS -Service die Option GuardDuty aus.
12. Wählen Sie als Ereignistyp die Option GuardDutyFinding aus.
13. Wählen Sie Weiter aus.
14. Bei Zieltypen wählen Sie AWS -Service aus.
15. Wählen Sie für Ziel auswählen das SNS-Thema und für Thema den Namen des SNS-Themas, das Sie zuvor erstellt haben.
16. Wählen Sie im Abschnitt Zusätzliche Einstellungen unter Zieleingabe konfigurieren die Option Eingabe-Transformer.

    Durch das Hinzufügen eines Eingangstransformators werden die gesendeten JSON-Suchdaten GuardDuty in eine für Menschen lesbare Nachricht formatiert.
17. Wählen Sie Configure input transformer (Eingabetransformator konfigurieren).
18. Fügen Sie im Abschnitt Ziel-Eingabe-Transformer für Eingabepfad den folgenden Code ein:

```
{
  "severity": "$.detail.severity",
  "Finding_ID": "$.detail.id",
  "Finding_Type": "$.detail.type",
  "region": "$.region",
  "Finding_Description": "$.detail.description"
}
```

19. Um die E-Mail zu formatieren, fügen Sie für Template den folgenden Code ein und achten Sie darauf, den roten Text durch die Werte zu ersetzen, die Ihrer Region entsprechen:

```
"You have a severity <severity> GuardDuty finding type <Finding_Type> in the
 <region> region."
"Finding Description:"
"<Finding_Description>."
```

```
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=<region>#/findings?search=id%3D<Finding_ID>"
```

20. Wählen Sie Bestätigen aus.
21. Wählen Sie Weiter aus.
22. (Optional) Geben Sie ein oder mehrere Tags für die Regel ein. Weitere Informationen finden Sie unter EventBridge Amazon-Tags im EventBridge Amazon-Benutzerhandbuch.
23. Wählen Sie Weiter aus.
24. Überprüfen Sie die Details der Regel und wählen Sie dann Regel erstellen aus.
25. (Optional) Testen Sie Ihre neue Regel, indem Sie anhand des in Schritt 2 beschriebenen Prozesses Beispiel-Erkenntnisse generieren. Sie erhalten für jede generierte Beispiel-Erkenntnis eine E-Mail.

Nächste Schritte

Wenn Sie die Nutzung fortsetzen GuardDuty, werden Sie verstehen, welche Arten von Ergebnissen für Ihre Umgebung relevant sind. Wenn Sie eine neue Erkenntnis erhalten, können Sie Informationen, einschließlich Empfehlungen zur Problembehebung, zu dieser Erkenntnis finden, indem Sie in der Beschreibung der Erkenntnis im Bereich mit den Erkenntnisdetails die Option Weitere Informationen auswählen oder indem Sie unter nach dem Namen der Erkenntnis in GuardDuty Typen finden suchen.

Die folgenden Funktionen helfen Ihnen bei der Feinabstimmung, GuardDuty sodass die relevantesten Ergebnisse für Ihre AWS Umgebung bereitgestellt werden können:

- Um Ergebnisse auf einfache Weise nach bestimmten Kriterien wie Instanz-ID, Konto-ID, S3-Bucket-Name und mehr zu sortieren, können Sie darin Filter erstellen und speichern GuardDuty. Weitere Informationen finden Sie unter Ergebnisse filtern in GuardDuty.
- Wenn Sie Erkenntnisse zu erwartetem Verhalten in Ihrer Umgebung erhalten, können Sie die Erkenntnisse anhand der Kriterien, die Sie mit Unterdrückungsregeln definieren, automatisch archivieren.
- Um zu verhindern, dass Ergebnisse anhand einer Teilmenge vertrauenswürdiger IPs generiert werden, oder um GuardDuty Monitor-IPs außerhalb des normalen Überwachungsbereichs zu platzieren, können Sie Listen vertrauenswürdiger IP-Adressen und Bedrohungen einrichten.

GuardDuty grundlegende Datenquellen

GuardDuty verwendet die grundlegenden Datenquellen, um die Kommunikation mit bekannten bösartigen Domänen und IP-Adressen zu erkennen und potenziell anomales Verhalten und unbefugte Aktivitäten zu identifizieren. Bei der Übertragung von diesen Quellen zu GuardDuty werden alle Protokolldaten verschlüsselt. GuardDuty extrahiert verschiedene Felder aus diesen Protokollquellen für die Profilerstellung und die Erkennung von Anomalien und verwirft diese Protokolle anschließend.

Wenn Sie die Aktivierung GuardDuty zum ersten Mal in einer Region durchführen, gibt es eine kostenlose 30-Tage-Testversion, die die Bedrohungserkennung für alle grundlegenden Datenquellen umfasst. Während dieser kostenlosen Testversion können Sie die geschätzte monatliche Nutzung, aufgeschlüsselt nach jeder grundlegenden Datenquelle, überwachen. Als delegiertes GuardDuty Administratorkonto können Sie sich die geschätzten monatlichen Nutzungskosten anzeigen lassen, aufgeschlüsselt nach jedem Mitgliedskonto, das zu Ihrer Organisation gehört und aktiviert wurde. GuardDuty Nach Ablauf der 30-Tage-Testversion können Sie Informationen AWS Billing zu den Nutzungskosten abrufen.

Für den GuardDuty Zugriff auf Ereignisse und Protokolle aus diesen grundlegenden Datenquellen fallen keine zusätzlichen Kosten an.

Nachdem Sie Ihre aktiviert GuardDuty haben AWS-Konto, beginnt sie automatisch mit der Überwachung der in den folgenden Abschnitten erläuterten Protokollquellen. Sie müssen nichts anderes aktivieren, um mit der Analyse und Verarbeitung dieser Datenquellen zu beginnen, um entsprechende Sicherheitsergebnisse zu generieren. GuardDuty

Themen

- AWS CloudTrail Verwaltungsereignisse
- VPC Flow Logs
- Route53 Resolver DNS-Abfrageprotokolle

AWS CloudTrail Verwaltungsereignisse

AWS CloudTrail bietet Ihnen einen Verlauf der AWS API-Aufrufe für Ihr Konto, einschließlich API-Aufrufe, die mithilfe der AWS SDKs AWS-Managementkonsole, der Befehlszeilentools und bestimmter AWS Dienste getätigt wurden. CloudTrail hilft Ihnen auch dabei, zu ermitteln, welche Benutzer und Konten AWS APIs für Dienste aufgerufen haben CloudTrail, die Quell-IP-Adresse,

von der aus die Aufrufe aufgerufen wurden, und den Zeitpunkt, zu dem die Aufrufe aufgerufen wurden. Weitere Informationen finden Sie unter Was ist AWS CloudTrail im AWS CloudTrail - Benutzerhandbuch.

GuardDuty überwacht CloudTrail Verwaltungsereignisse, auch bekannt als Ereignisse auf der Kontrollebene. Diese Ereignisse bieten Einblick in Verwaltungsvorgänge, die an Ressourcen in Ihrem Unternehmen ausgeführt werden AWS-Konto.

Im Folgenden finden Sie Beispiele für CloudTrail Verwaltungsereignisse, die GuardDuty überwacht werden:

- Konfiguration der Sicherheit (`AttachRolePolicy`IAM-API-Operationen)
- Konfigurieren von Regeln für die Datenweiterleitung (z. B. `CreateSubnet`-API-Vorgänge von Amazon EC2)
- Einrichtung der Protokollierung (AWS CloudTrail `CreateTrail`API-Operationen)

Wenn Sie diese GuardDuty Option aktivieren, werden CloudTrail Verwaltungsereignisse direkt CloudTrail über einen unabhängigen und duplizierten Ereignisstrom verarbeitet und Ihre CloudTrail Ereignisprotokolle analysiert.

GuardDuty verwaltet Ihre CloudTrail Ereignisse nicht und wirkt sich auch nicht auf Ihre vorhandenen CloudTrail Konfigurationen aus. Ebenso haben Ihre CloudTrail Konfigurationen keinen Einfluss darauf, wie GuardDuty die Ereignisprotokolle genutzt und verarbeitet werden. Verwenden Sie die CloudTrail Servicekonsole oder API, um den Zugriff auf Ihre CloudTrail Ereignisse und deren Aufbewahrung zu verwalten. Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Wie GuardDuty geht man mit AWS CloudTrail globalen Ereignissen um

Bei den meisten AWS Diensten werden CloudTrail Ereignisse dort aufgezeichnet, AWS-Region wo sie erstellt wurden. Für globale Dienste wie AWS Identity and Access Management (IAM), AWS - Security-Token-Service (AWS STS), Amazon Simple Storage Service (Amazon S3) CloudFront, Amazon und Amazon Route 53 (Route 53) werden Ereignisse nur in der Region generiert, in der sie auftreten, aber sie haben globale Bedeutung.

Wenn GuardDuty CloudTrail Global Service Events (GSE) mit Sicherheitswerten wie Netzwerkkonfigurationen oder Benutzerberechtigungen verwendet werden, repliziert es diese Ereignisse und verarbeitet sie in jeder Region, in der Sie sie aktiviert haben. GuardDuty Dieses

Verhalten hilft dabei, Benutzer- und Rollenprofile in jeder Region zu GuardDuty verwalten, was für die Erkennung ungewöhnlicher Ereignisse von entscheidender Bedeutung ist.

> **Note**
>
> Bei Ergebnissen, die aus diesen globalen Serviceereignissen generiert wurden, kann sich der Wert „Region“ im Ergebnis von der Region unterscheiden, in der die GuardDuty Erkennung erfolgt. Beispielsweise kann ein Ergebnis `us-east-1` als Region angezeigt werden, auch wenn GuardDuty die Erkennung in einer anderen Region erfolgt.

Wir empfehlen Ihnen, alle AWS-Regionen verfügbaren GuardDuty Optionen in Ihrem zu aktivieren AWS-Konto. Auch wenn Sie in bestimmten Regionen keine Ressourcen bereitgestellt haben, GuardDuty trägt die Aktivierung dazu bei, Ihr Konto vor potenziellen Bedrohungen zu schützen. Bedrohungsakteure können potenziell Angriffe über globale Dienste (wie IAM oder Amazon CloudFront) starten. AWS STS Sie können versuchen, nicht autorisierte Ressourcen zu erstellen, um Regionen auszunutzen, in denen Sie nur begrenzt präsent sind. GuardDuty verarbeitet globale Serviceereignisse in allen Regionen, in denen Sie den Service aktiviert haben, einschließlich der Standard- und Opt-in-Regionen. Auf diese Weise GuardDuty können potenziell verdächtige Aktivitäten in Ihren Regionen erkannt werden AWS-Konto, auch in Regionen, in denen Sie Ressourcen nicht aktiv nutzen.

VPC Flow Logs

Mit dem Feature VPC-Flow-Protokollen von Amazon VPC erfassen Sie Informationen zum IP-Datenverkehr zu und von Netzwerkschnittstellen, die mit Amazon Elastic Compute Cloud (Amazon EC2)-Instances in Ihrer AWS -Umgebung verbunden sind.

Wenn Sie es aktivieren GuardDuty, beginnt es sofort mit der Analyse von VPC-Flow-Protokolldaten von Amazon EC2 EC2-Instances in Ihrem Konto. GuardDuty verbraucht diese Daten über einen unabhängigen und duplizierten Stream von Flow-Logs. Sie müssen in Ihrem Konto keine VPC-Flow-Logs erstellen oder konfigurieren, GuardDuty um auf diese Daten zugreifen zu können. Dieser Prozess wirkt sich nicht auf ggf. vorhandene Flow-Protokollkonfigurationen aus.

Lambda Protection

Lambda Protection ist eine optionale Erweiterung für Amazon GuardDuty. Derzeit umfasst Lambda Network Activity Monitoring Amazon-VPC-Flow-Protokolle von allen Lambda-Funktionen

für Ihr Konto, auch solche, die kein VPC-Netzwerk verwenden. Um Ihre Lambda-Funktion vor potenziellen Sicherheitsbedrohungen zu schützen, müssen Sie Lambda Protection in Ihrem GuardDuty Konto konfigurieren. Weitere Informationen finden Sie unter Lambda Protection.

GuardDuty Überwachung der Laufzeit

Wenn Sie den Security Agent (entweder manuell oder über GuardDuty) in EKS Runtime Monitoring oder Runtime Monitoring for EC2-Instances verwalten und derzeit auf einer Amazon EC2 EC2-Instance bereitgestellt GuardDuty ist und diese Gesammelte Laufzeit-Ereignistypen von dieser Instance empfängt, GuardDuty wird Ihnen die Analyse der VPC-Flow-Logs von dieser Amazon EC2 EC2-Instance nicht in Rechnung gestellt. AWS-Konto Dies trägt dazu bei, doppelte Nutzungskosten für das Konto GuardDuty zu vermeiden.

GuardDuty verwaltet Ihre Flow-Logs nicht und macht sie auch nicht in Ihrem Konto zugänglich. Damit Sie den Zugriff und die Aufbewahrung Ihrer Flow-Protokolle verwalten können, müssen Sie das Feature VPC-Flow-Protokolle konfigurieren.

Route53 Resolver DNS-Abfrageprotokolle

Wenn Sie AWS DNS-Resolver für Ihre Amazon EC2 EC2-Instances verwenden (Standardeinstellung), GuardDuty können Sie über die internen DNS-Resolver auf Ihre Anfrage und Antwort Route53 Resolver DNS-Abfrageprotokolle zugreifen und diese verarbeiten. AWS Wenn Sie einen anderen DNS-Resolver wie OpenDNS oder GoogleDNS verwenden oder wenn Sie Ihre eigenen DNS-Resolver einrichten, GuardDuty können Sie nicht auf Daten aus dieser Datenquelle zugreifen und diese verarbeiten.

Wenn Sie es aktivieren GuardDuty, beginnt es sofort mit der Analyse Ihrer Route53 Resolver-DNS-Abfrageprotokolle aus einem unabhängigen Datenstrom. Dieser Datenstrom ist von den Daten getrennt, die über das Feature Route-53-Resolver-Abfrageprotokollierung bereitgestellt werden. Die Konfiguration dieser Funktion hat keinen Einfluss auf die Analyse. GuardDuty

> **Note**
>
> GuardDuty unterstützt nicht die Überwachung von DNS-Protokollen für Amazon EC2 EC2-Instances, auf denen gestartet wurde, AWS Outposts da die Amazon Route 53 Resolver Abfrageprotokollierungsfunktion in dieser Umgebung nicht verfügbar ist.

GuardDuty Erweiterte Bedrohungserkennung

GuardDuty Extended Threat Detection erkennt automatisch mehrstufige Angriffe, die sich über Datenquellen, mehrere AWS Ressourcentypen und einen Zeitraum erstrecken, innerhalb eines AWS-Konto. Mit dieser Funktion GuardDuty konzentriert es sich auf die Abfolge mehrerer Ereignisse, die es beobachtet, indem es verschiedene Arten von Datenquellen überwacht. Extended Threat Detection korreliert diese Ereignisse, um Szenarien zu identifizieren, die sich als potenzielle Bedrohung für Ihre AWS Umgebung darstellen, und generiert dann eine Ermittlung der Angriffssequenz.

Themen

- Beispiele für Bedrohungsszenarien mit Angriffssequenz
- Funktionsweise
- Aktivierung von Schutzplänen zur Maximierung der Bedrohungserkennung
- Erweiterte Bedrohungserkennung in der Konsole GuardDuty
- Die Ergebnisse der Angriffssequenz verstehen und verwalten
- Weitere Ressourcen

Beispiele für Bedrohungsszenarien mit Angriffssequenz

Extended Threat Detection deckt Bedrohungsszenarien ab, die mit dem Missbrauch von AWS Anmeldeinformationen, Datenkompromittierungsversuchen in Amazon S3 S3-Buckets und der Kompromittierung von Containern und Kubernetes-Ressourcen in Amazon EKS-Clustern einhergehen. Ein einziger Befund kann eine gesamte Angriffssequenz umfassen. In der folgenden Liste werden beispielsweise die Szenarien beschrieben, bei denen Folgendes erkannt werden GuardDuty könnte:

Beispiel 1 — Datenkompromittierung von AWS Anmeldedaten und Amazon S3 S3-Bucket-Daten

- Ein Bedrohungsakteur, der sich unbefugten Zugriff auf einen Rechen-Workload verschafft.
- Der Akteur führt dann eine Reihe von Aktionen durch, z. B. die Eskalation von Rechten und die Herstellung von Persistenz.
- Schließlich exfiltriert der Akteur Daten aus einer Amazon S3 S3-Ressource.

Beispiel 2 — Amazon EKS-Cluster-Kompromiss

- Ein Bedrohungsakteur versucht, eine Container-Anwendung innerhalb eines Amazon EKS-Clusters auszunutzen.
- Der Akteur verwendet diesen kompromittierten Container, um Token für privilegierte Dienstkonten zu erhalten.
- Der Akteur nutzt dann diese erhöhten Rechte, um über Pod-Identitäten auf sensible Kubernetes-Geheimnisse oder AWS -Ressourcen zuzugreifen.

GuardDuty Betrachtet aufgrund der Art der damit verbundenen Bedrohungsszenarien alle Szenarien als kritisch. Arten der Suche nach Angriffssequenzen

Das folgende Video zeigt, wie Sie Extended Threat Detection verwenden können.

Vorführung von Amazon GuardDuty Extended Threat Detection

Funktionsweise

Wenn Sie Amazon GuardDuty in Ihrem Konto in einem bestimmten Bereich aktivieren AWS-Region, ist Extended Threat Detection standardmäßig ebenfalls aktiviert. Mit der Nutzung

von Extended Threat Detection sind keine zusätzlichen Kosten verbunden. Standardmäßig werden alle Grundlegende Datenquellen Ereignisse miteinander korreliert. Wenn Sie jedoch mehr GuardDuty Schutzpläne wie S3 Protection, EKS Protection und Runtime Monitoring aktivieren, werden dadurch zusätzliche Arten der Erkennung von Angriffssequenzen eröffnet, da die Bandbreite der Ereignisquellen erweitert wird. Dies kann möglicherweise zu einer umfassenderen Bedrohungsanalyse und zur besseren Erkennung von Angriffssequenzen beitragen. Weitere Informationen finden Sie unter Aktivierung von Schutzplänen zur Maximierung der Bedrohungserkennung.

GuardDuty korreliert mehrere Ereignisse, einschließlich API-Aktivitäten und GuardDuty -Ergebnisse. Diese Ereignisse werden als Signale bezeichnet. Manchmal kann es in Ihrer Umgebung Ereignisse geben, die sich für sich genommen nicht als eindeutige potenzielle Bedrohung darstellen. GuardDuty bezeichnet sie als schwache Signale. GuardDuty Identifiziert mit Extended Threat Detection, wenn eine Abfolge mehrerer Aktionen auf eine potenziell verdächtige Aktivität zurückzuführen ist, und generiert eine Erkennung der Angriffssequenz in Ihrem Konto. Diese vielfältigen Aktionen können schwache Signale und bereits festgestellte GuardDuty Ergebnisse in Ihrem Konto beinhalten.

> **Note**
>
> Bei der Zuordnung von Ereignissen zu Angriffssequenzen berücksichtigt Extended Threat Detection archivierte Ergebnisse nicht, auch solche, die aufgrund von Unterdrückungsregeln automatisch archiviert werden. Dieses Verhalten stellt sicher, dass nur aktive, relevante Signale zur Erkennung der Angriffssequenz beitragen. Um sicherzustellen, dass Sie davon nicht betroffen sind, überprüfen Sie die bestehenden Unterdrückungsregeln in Ihrem Konto. Weitere Informationen finden Sie unter Verwendung von Unterdrückungsregeln mit Extended Threat Detection.

GuardDuty dient außerdem der Identifizierung potenzieller laufender oder kürzlich aufgetretener Angriffe (innerhalb eines fortlaufenden Zeitfensters von 24 Stunden) in Ihrem Konto. Ein Angriff könnte beispielsweise damit beginnen, dass sich ein Akteur unbeabsichtigt Zugriff auf eine Rechenlast verschafft. Der Akteur würde dann eine Reihe von Schritten ausführen, darunter die Aufzählung, die Eskalation von Rechten und die Exfiltration von Anmeldeinformationen. AWS Diese Anmeldeinformationen könnten möglicherweise für weitere Sicherheitslücken oder für den böswilligen Zugriff auf Daten verwendet werden.

Aktivierung von Schutzplänen zur Maximierung der Bedrohungserkennung

Die erweiterte Bedrohungserkennung wird automatisch für alle GuardDuty Konten aktiviert und wertet standardmäßig Signale aller im Konto aktivierten Schutzpläne aus. GuardDuty Grundlegende Datenquellen liefern wichtige Signale für die Erkennung verschiedener Angriffssequenzen. Mit einer grundlegenden Bedrohungserkennung GuardDuty kann beispielsweise eine potenzielle Angriffssequenz anhand der Aktivität zur Erkennung von IAM-Rechten auf Amazon S3 S3-APIs identifiziert und nachfolgende Änderungen der S3-Steuerungsebene erkannt werden, z. B. Änderungen, die die Bucket-Ressourcenrichtlinie toleranter machen. Andere Angriffssequenzen erfordern jedoch erweiterte Signale, die nur in erweiterten Schutzplänen wie Runtime Monitoring, S3 Protection und EKS Audit Log Monitoring verfügbar sind.

Themen

- Erkennung von Angriffssequenzen in Amazon EKS-Clustern
- Erkennung von Angriffssequenzen in Amazon S3 S3-Buckets
- Erkennung von Angriffssequenzen in Amazon ECS-Clustern
- Erkennung von Angriffssequenzen in Amazon EC2 EC2-Instanzgruppen

Erkennung von Angriffssequenzen in Amazon EKS-Clustern

GuardDuty Korrelierte mehrere Sicherheitssignale zwischen EKS-Auditprotokollen, dem Laufzeitverhalten von Prozessen und AWS API-Aktivitäten, um ausgeklügelte Angriffsmuster zu erkennen. Um von Extended Threat Detection for EKS zu profitieren, müssen Sie mindestens eine dieser Funktionen aktivieren — EKS-Schutz oder Runtime Monitoring (mit EKS-Add-on). EKS Protection überwacht die Aktivitäten auf der Kontrollebene anhand von Auditprotokollen, während Runtime Monitoring das Verhalten innerhalb von Containern beobachtet.

Für eine maximale Abdeckung und eine umfassende Bedrohungserkennung GuardDuty empfiehlt es sich, beide Schutzpläne zu aktivieren. Zusammen bieten sie einen vollständigen Überblick über Ihre EKS-Cluster und ermöglichen so GuardDuty die Erkennung komplexer Angriffsmuster. Es kann beispielsweise eine anomale Bereitstellung eines privilegierten Containers (erkannt mit EKS Protection) identifizieren, gefolgt von Persistenzversuchen, Krypto-Mining und Reverse-Shell-Erstellung innerhalb dieses Containers (erkannt mit Runtime Monitoring). GuardDuty stellt diese zusammenhängenden Ereignisse als einen einzigen Befund mit kritischem Schweregrad dar, der

so genannten. AttackSequence:EKS/CompromisedCluster Wenn Sie beide Schutzpläne aktivieren, deckt die Ermittlung der Angriffssequenz die folgenden Bedrohungsszenarien ab:

- Kompromittierung von Containern, auf denen anfällige Webanwendungen laufen
- Unberechtigter Zugriff durch falsch konfigurierte Anmeldeinformationen
- Versuche, Rechte zu eskalieren
- Verdächtige API-Anfragen
- Versuche, böswillig auf Daten zuzugreifen

Die folgende Liste enthält Einzelheiten darüber, wann diese speziellen Schutzpläne einzeln aktiviert werden:

EKS-Schutz

Durch die Aktivierung von EKS GuardDuty Protection können Angriffssequenzen erkannt werden, die Aktivitäten der Amazon EKS-Cluster-Steuerebene betreffen. Auf diese Weise können GuardDuty EKS-Auditprotokolle und AWS API-Aktivitäten korreliert werden. GuardDuty Kann beispielsweise eine Angriffssequenz erkennen, bei der ein Akteur versucht, unbefugt auf Cluster-Geheimnisse zuzugreifen, die RBAC-Berechtigungen (RBAC) von Kubernetes ändert und privilegierte Pods erstellt. Weitere Informationen zur Aktivierung dieses Schutzplans finden Sie unter. EKS-Schutz

Laufzeitüberwachung für Amazon EKS

Die Aktivierung von Runtime Monitoring für Amazon EKS-Cluster bietet die GuardDuty Möglichkeit, die Erkennung von EKS-Angriffssequenzen mit Transparenz auf Container-Ebene zu verbessern. Auf diese Weise GuardDuty können potenzielle bösartige Prozesse, verdächtiges Laufzeitverhalten und die mögliche Ausführung von Malware erkannt werden. GuardDuty Kann beispielsweise eine Angriffssequenz erkennen, bei der ein Container anfängt, verdächtiges Verhalten an den Tag zu legen, z. B. Krypto-Mining-Prozesse oder das Herstellen von Verbindungen zu bekannten bösartigen Endpunkten. Weitere Informationen zur Aktivierung dieses Schutzplans finden Sie unter. Laufzeitüberwachung

Wenn Sie EKS-Schutz oder Runtime Monitoring nicht aktivieren, können keine individuellen Arten der Suche nach EKS-Schutz oder generiert GuardDuty werdenBei der Laufzeitüberwachung werden Typen gefunden. GuardDuty Wird daher nicht in der Lage sein, mehrstufige Angriffssequenzen zu erkennen, die zugehörige Ergebnisse beinhalten.

Erkennung von Angriffssequenzen in Amazon S3 S3-Buckets

Durch die Aktivierung von S3 Protection GuardDuty können Angriffssequenzen erkannt werden, bei denen versucht wird, Daten in Ihren Amazon S3 S3-Buckets zu kompromittieren. Ohne S3-Schutz GuardDuty kann erkannt werden, wenn Ihre S3-Bucket-Ressourcenrichtlinie zu freizügig wird. Wenn Sie S3 Protection aktivieren, ist es in der Lage GuardDuty , potenzielle Datenexfiltrationsaktivitäten zu erkennen, die auftreten können, nachdem Ihr S3-Bucket zu freizügig geworden ist.

Wenn S3 Protection nicht aktiviert ist, können keine GuardDuty individuellen Daten generiert werden. S3-Schutztypen finden Daher GuardDuty wird es nicht möglich sein, mehrstufige Angriffssequenzen zu erkennen, die zugehörige Ergebnisse beinhalten. Weitere Informationen zur Aktivierung dieses Schutzplans finden Sie unterS3-Schutz.

Erkennung von Angriffssequenzen in Amazon ECS-Clustern

GuardDuty kann Angriffssequenzen wie bösartige Prozesse, Verbindungen zu böswilligen Endpunkten oder Crypto-Mining-Verhalten innerhalb von ECS-Containern identifizieren. Durch die Korrelation verschiedener Signale in Bezug auf Netzwerkaktivität, Prozesslaufzeitverhalten und AWS API-Aktivität GuardDuty können komplexe Angriffsmuster identifiziert werden, die bei einzelnen Erkennungen möglicherweise übersehen werden, und der gesamte Angriffsvektor abgebildet werden.

GuardDuty stellt diese zusammenhängenden Ereignisse in Form eines einzigen Befundes mit kritischem Schweregrad dar. `AttackSequence:ECS/CompromisedCluster` Die Ermittlung der Angriffssequenz deckt die folgenden Bedrohungsszenarien ab:

- Kompromittierung von Containern, die anfällige Dienste ausführen
- Unbefugte Ausführung verdächtiger Tools, Malware oder Cryptomining-Prozesse
- Versuche, Rechte zu erweitern
- Kommunikation mit verdächtigen Endpunkten

> **Important**
>
> Extended Threat Detection for ECS erfordert je nach ECS-Infrastrukturtyp Runtime Monitoring für Fargate oder EC2. Runtime Monitoring beobachtet das Verhalten in ECS-Containern, die sowohl auf Fargate- als auch auf EC2-Instances ausgeführt werden. ECS auf verwalteten EC2-Instances wird nicht unterstützt.

Erkennung von Angriffssequenzen in Amazon EC2 EC2-Instanzgruppen

GuardDuty kann Angriffssequenzen identifizieren, die einzelne Instances oder Gruppen von Instances betreffen, die gemeinsame Attribute wie Auto Scaling Scaling-Gruppen, IAM-Instanzprofile, Startvorlagen, CloudFormation Stacks, AMIs oder VPC-IDs aufweisen. Diese Instances können verdächtige Verhaltensweisen wie bösartige Prozesse, Verbindungen zu böswilligen Endpunkten, Krypto-Mining oder eine abnormale Verwendung von EC2-Instance-Anmeldeinformationen aufweisen.

Bei der Suche nach der Angriffssequenz werden die folgenden Bedrohungsszenarien erkannt:

- Gefährdung von Instanzen, auf denen anfällige Dienste ausgeführt werden
- Verwendung von Amazon EC2 EC2-Instance-Anmeldeinformationen, die über IMDS von außerhalb des AWS Kontos abgerufen wurden, für das die Anmeldeinformationen ausgestellt wurden
- Verwendung als Infrastruktur für Angriffe wie Proxy, Scannen oder Denial-of-Service
- Unbefugte Ausführung verdächtiger Tools, Malware oder Cryptomining-Prozesse
- Kommunikation mit verdächtigen Endpunkten

Extended Threat Detection hilft bei der Identifizierung dieser Bedrohungen. GuardDuty stellt diese zusammenhängenden Ereignisse in Form eines einzigen Befundes mit kritischem Schweregrad dar, dem so genannten. `AttackSequence:EC2/CompromisedInstanceGroup`

Um die Erkennungsfunktionen von Extended Threat Detection für EC2 zu verbessern, aktivieren Sie Runtime Monitoring. Die Kombination aus Basic GuardDuty, das die Netzwerkaktivität überwacht, CloudTrail und Runtime Monitoring, das Prozessverhalten und Systemaufrufen innerhalb von Instances beobachtet, ermöglicht eine umfassendere Bedrohungserkennung. Diese integrierte Überwachung ermöglicht GuardDuty die Erkennung ausgeklügelter Angriffssequenzen wie unbefugten Zugriff durch falsch konfigurierte Anmeldeinformationen, Versuche zur Eskalation von Rechten und unberechtigtem Zugriff auf vertrauliche Daten. Durch die Korrelation dieser verschiedenen Signale GuardDuty können komplexe Angriffsmuster identifiziert werden, die bei einzelnen Erkennungen möglicherweise übersehen werden, und der gesamte Angriffsvektor abgebildet werden.

Erweiterte Bedrohungserkennung in der Konsole GuardDuty

Standardmäßig wird auf der Seite „Erweiterte Bedrohungserkennung“ in der GuardDuty Konsole der Status „Aktiviert“ angezeigt. Bei der grundlegenden Bedrohungserkennung steht der

Status dafür, dass eine potenzielle Angriffssequenz erkannt werden GuardDuty kann, die IAM-Rechteerkennungsaktivitäten auf Amazon S3 S3-APIs und die Erkennung nachfolgender Änderungen der S3-Steuerebene umfasst.

Gehen Sie wie folgt vor, um die Seite Extended Threat Detection in der Konsole aufzurufen: GuardDuty

1. Sie können die GuardDuty Konsole unter öffnen https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im linken Navigationsbereich Extended Threat Detection aus.

   Diese Seite enthält Einzelheiten zu den Bedrohungsszenarien, die von Extended Threat Detection abgedeckt werden.
3. Sehen Sie sich auf der Seite Extended Threat Detection den Abschnitt Verwandte Schutzpläne an. Wenn Sie spezielle Schutzpläne aktivieren möchten, um den Schutz vor Bedrohungserkennung in Ihrem Konto zu erhöhen, wählen Sie die Option Konfigurieren für diesen Schutzplan aus.

Die Ergebnisse der Angriffssequenz verstehen und verwalten

Die Ergebnisse der Angriffssequenz sind genau wie andere GuardDuty Ergebnisse in Ihrem Konto. Sie können sie auf der Seite mit den Ergebnissen in der GuardDuty Konsole einsehen. Informationen zum Anzeigen von Ergebnissen finden Sie unterSeite mit den Ergebnissen in der GuardDuty Konsole.

Ähnlich wie bei anderen GuardDuty Ergebnissen werden auch die Ergebnisse der Angriffssequenz automatisch an Amazon gesendet EventBridge. Basierend auf Ihren Einstellungen werden die Ergebnisse der Angriffssequenz auch an ein Veröffentlichungsziel (Amazon S3 S3-Bucket) exportiert. Informationen zum Festlegen eines neuen Veröffentlichungsziels oder zum Aktualisieren eines vorhandenen finden Sie unterGenerierte Ergebnisse nach Amazon S3 exportieren.

Weitere Ressourcen

Lesen Sie die folgenden Abschnitte, um mehr über Angriffssequenzen zu erfahren:

- Nachdem Sie sich mit der erweiterten Bedrohungserkennung und den Angriffssequenzen vertraut gemacht haben, können Sie anhand der unter beschriebenen Schritte Beispiele für die Suche nach Angriffssequenzen generierenBeispielerkenntnisse.
- Erfahren Sie mehr über Arten der Suche nach Angriffssequenzen.

- Überprüfen Sie die Ergebnisse und untersuchen Sie die Einzelheiten der Ergebnisse im Zusammenhang mitEinzelheiten zur Suche nach der Angriffssequenz.
- Priorisieren und beheben Sie die Arten der Erkennung von Angriffssequenzen, indem Sie die Schritte für die zugehörigen betroffenen Ressourcen unter befolgen. Behebung von Erkenntnissen

Schutzpläne konfigurieren

Auf der Seite Schutzpläne in der GuardDuty Konsole werden alle Schutzplankonfigurationen auf einer einzigen Seite zusammengefasst. Sie können Schutzpläne aktivieren oder deaktivieren, Einstellungen zur automatischen Aktivierung für AWS Organizations Konten konfigurieren und Statistiken zu Mitgliedskonten von einem zentralen Ort aus einsehen.

-Übersicht

Die einheitliche Seite mit den Schutzplänen macht es überflüssig, zur Konfiguration zu den Seiten der einzelnen Schutzpläne zu navigieren. In der Konsolennavigation wird ein einziger Link zu Schutzplänen angezeigt.

Auf der Seite werden Schutzpläne in der folgenden Reihenfolge angezeigt:

1. Grundlegend GuardDuty — Aktiviert oder deaktiviert GuardDuty und konfiguriert die automatische Aktivierung für AWS Organizations Konten.
2. S3-Schutz — Überwachen Sie Amazon S3 S3-Datenereignisse auf potenzielle Bedrohungen für Ihre Daten.
3. Laufzeitüberwachung — Überwachen Sie Ereignisse auf Betriebssystemebene für EKS-, ECS- und EC2-Workloads.
4. EKS-Auditprotokolle — Überwachen Sie die Amazon EKS-Auditprotokolle auf potenzielle Bedrohungen für Ihre Cluster.
5. RDS-Schutz — Überwachen Sie die RDS-Anmeldeaktivitäten auf potenzielle Bedrohungen für Ihre Datenbanken.
6. Lambda-Schutz — Überwachen Sie die Netzwerkaktivität der Lambda-Funktion auf potenzielle Bedrohungen.

Jeder Schutzplan enthält die folgenden Informationen:

- Funktionsstatus (Aktiviert oder Nicht aktiviert)
- Auto-enable Status für AWS Organizations Konten
- AWS Organizations Konten, Mitgliederstatistiken

Konfiguration aller Schutzpläne

Gehen Sie wie folgt vor, um Schutzpläne auf der einheitlichen Seite zu konfigurieren:

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Schutzpläne aus.
3. Wählen Sie Alle Aktivierungen konfigurieren aus. Alle Schutzplan-Container wechseln in den Bearbeitungsmodus.
4. Nehmen Sie Änderungen an einem oder allen Schutzplänen vor. Für jeden Plan können Sie die Funktion ein- oder ausschalten und die Einstellung für die automatische Aktivierung für Organisationskonten konfigurieren.
5. Klicken Sie auf Save all. Ein Bestätigungsfenster wird angezeigt, das alle Änderungen zusammenfasst, einschließlich des Funktionsnamens, des Status und des Werts für die automatische Aktivierung für jeden geänderten Plan.
6. Überprüfen Sie die Änderungen und wählen Sie Bestätigen und speichern. Alle Änderungen werden stapelweise gespeichert.

Auto-enable Optionen

Jeder Schutzplan bietet die folgenden Optionen zur automatischen Aktivierung von Unternehmenskonten:

Für alle Konten aktivieren

Aktivieren Sie die Funktion für alle aktiven GuardDuty Konten in der Organisation. Dies schließt neue Konten ein, die der Organisation beitreten.

Für neue Konten aktivieren

Dies gilt für alle neuen Konten, wenn sie der Organisation hinzugefügt werden.

Nicht auto aktivieren

Die Funktion wird nicht automatisch für Organisationskonten aktiviert.

Für den GuardDutyFoundational-Container verwenden die Optionen zur automatischen Aktivierung einen AWS Organizations-spezifischen Wortlaut:

- Für alle AWS Organizations Konten aktivieren — Aktiviert GuardDuty für alle aktiven Konten in Ihrem. AWS Organizations
- Für neue AWS Organizations Konten aktivieren — Dies gilt für alle neuen Konten, wenn sie zu Ihren hinzugefügt werden AWS Organizations.

Konfiguration der Laufzeitüberwachung

Der Runtime Monitoring-Container hat eine übergeordnete und untergeordnete Struktur mit den folgenden Unterfunktionen:

- Laufzeitüberwachung (EKS)
- Laufzeitüberwachung (ECS)
- Laufzeitüberwachung (EC2)

Die Einstellung Runtime Monitoring Infrastructure wird in einem erweiterbaren Bereich angezeigt. Diese Einstellung ist erforderlich, damit Runtime Monitoring für EKS, ECS und EC2 funktioniert, bietet jedoch keinen Schutz für sich.

Bidirektionale Einschränkungen

Die Unterfunktionen von Runtime Monitoring und die Infrastruktur stehen in den folgenden Beziehungen zueinander:

Aktivieren Sie eine Unterfunktion

: Aktiviert automatisch die Runtime Monitoring Infrastructure, falls sie deaktiviert wurde.

Deaktiviert eine Unterfunktion

: Keine Auswirkung auf die Runtime Monitoring Infrastructure.

Aktivieren Sie die Runtime Monitoring-Infrastruktur

: Keine Auswirkung auf Unterfunktionen.

Deaktivieren Sie die Runtime Monitoring Infrastructure

: Deaktiviert alle Unterfunktionen.

Für Einstellungen zur automatischen Aktivierung gelten die folgenden Einschränkungen:

Automatische Aktivierung einer Unterfunktion aktivieren

Die Runtime Monitoring Infrastructure entspricht immer dem Maximum aller Unterfunktionen.

Reduzieren Sie die automatische Aktivierung einer Unterfunktion

Die Runtime Monitoring Infrastructure berechnet das neue Maximum aller Unterfunktionen neu.

Erhöhen Sie die automatische Aktivierung der Runtime Monitoring Infrastructure

Keine Auswirkung auf Unterfunktionen.

Automatische Aktivierung der Lower Runtime Monitoring Infrastructure

Senkt alle Unterfunktionen, die den neuen übergeordneten Wert überschreiten, entsprechend.

> **Note**
>
> Eine Warnung wird angezeigt, wenn eine Unterfunktion einen anderen Wert als die Runtime Monitoring Infrastructure hat (entweder umschalten oder automatisch aktivieren). Wenn Sie nur die Runtime Monitoring Infrastructure aktivieren, gelangen Sie in den manuellen Modus ohne automatische Verwaltung des Security Agents. Aktivieren Sie Runtime Monitoring für EKS, ECS oder EC2, um den Security Agent automatisch für Ihre Workloads zu verwalten.

Statistiken zur Organisation

In jedem Schutzplan-Container werden Statistiken zu Mitgliedskonten angezeigt, aus denen hervorgeht, für wie viele Konten die Funktion aktiviert ist. Wenn Organisationsstatistiken noch nicht verfügbar sind (z. B. innerhalb der ersten 24 Stunden nach der Aktivierung), wird auf der Seite eine Statusanzeige für ausstehende Daten mit einer Meldung angezeigt, in der erklärt wird, dass Statistiken gesammelt werden.

Integration der Kontoseite

Die Schaltfläche Bearbeiten im Bereich Automatische Aktivierung auf der Seite Konten leitet Sie zur Seite Schutzpläne weiter, anstatt das ältere Konfigurationsmodal zu öffnen.

GuardDuty KI-Schutz

GuardDuty AI Protection erweitert die GuardDuty Bedrohungserkennung von Amazon auf darauf AWS aufbauende KI-Workloads. Wenn Sie den KI-Schutz aktivieren, GuardDuty werden AWS CloudTrail Datenereignisse von Amazon Bedrock, Amazon Bedrock AgentCore und Amazon SageMaker AI sowie Verwaltungsereignisse analysiert. AWS CloudTrail GuardDuty verwendet diese Daten, um potenziell verdächtige Aktivitäten zu erkennen, die auf Foundation-Modelle und die Anwendungen, die sie aufrufen, abzielen. Wenn GuardDuty eine potenzielle Bedrohung erkannt wird, generiert es eine oder mehrereArten der Suche nach KI-Schutz.

Wenn Sie den KI-Schutz aktivieren, GuardDuty kann es die folgenden Arten von Bedrohungen erkennen:

- Anomale Aufrufe von Amazon Bedrock- oder Amazon SageMaker AI-Modellen, die von der etablierten Basislinie für eine Identität oder ein Konto abweichen, z. B. Aufrufe von einer ungewöhnlichen IP-Adresse, einer ungewöhnlichen API oder einem ungewöhnlichen Modell.
- Cost-Harvesting-Angriffe, bei denen ein Bedrohungsakteur rechenintensive Eingaben an ein Amazon Bedrock- oder SageMaker Amazon-KI-Modell sendet, um den Token-Verbrauch und die Betriebskosten des Kontos in die Höhe zu treiben.
- Direkte Prompt-Injection-Versuche, bei denen ein Bedrohungsakteur eine böswillige Aufforderung erstellt, um ein Foundation-Modell dazu zu bringen, seine ursprünglichen Anweisungen zu ignorieren. Diese Erkennung erfordert Amazon Bedrock Guardrails und gilt nur für Amazon Bedrock-Workloads.

> **Note**
>
> Die Ergebnisarten, die in und generiert GuardDuty werden können, AWS-Region hängen davon ab, welche KI-Dienste in dieser Region verfügbar sind:
>
> - Für die Typen Impact:IAMUser/AnomalousModelInvocation und Impact:IAMUser/CostHarvesting Finding sind Amazon Bedrock oder Amazon SageMaker AI erforderlich. GuardDuty Generiert diese Ergebnistypen in Regionen, in denen Amazon Bedrock nicht verfügbar ist, ausschließlich anhand von Amazon SageMaker KI-Modellaufrufen.
> - Für den Impact:IAMUser/PromptInjection.Direct Findetyp ist Amazon Bedrock Guardrails erforderlich. Es ist nicht in Regionen verfügbar, in denen Amazon Bedrock Guardrails nicht unterstützt wird.

Die Liste der Regionen, in denen die einzelnen Suchtypen unterstützt werden, finden Sie unter. Region-specific Verfügbarkeit von Funktionen

> **Tip**
>
> Um den größtmöglichen Sicherheitsnutzen aus dem KI-Schutz herauszuholen, sollten Sie Amazon Bedrock Guardrails für schnelle Angriffe auf alle Konten in Ihrem Unternehmen durchsetzen. AWS Verwenden Sie die Richtlinien AWS Organizations von Amazon Bedrock, um diese Guardrail-Einstellungen zentral zu verwalten. Dies ermöglicht einen einheitlichen Schutz für alle Konten mit zentraler Steuerung und Verwaltung. Wenn eine Leitplanke für schnelle Angriffe durchgesetzt wird, werden umgehend GuardDuty Injection-Ergebnisse erzielt. Weitere Informationen finden Sie unter Impact:IAMUser/PromptInjection.Direct.

Um Bedrohungen für Ihre KI-Workloads zu erkennen, müssen Sie den KI-Schutz in Ihrem Konto aktivieren. GuardDuty Informationen zur Aktivierung des KI-Schutzes finden Sie unter Aktivierung des KI-Schutzes in Umgebungen mit mehreren Konten Für Umgebungen mit mehreren Konten oder. KI-Schutz für ein eigenständiges Konto aktivieren

Themen

- So funktioniert der KI-Schutz
- Preisgestaltung für KI-Schutz
- Zusätzliche Bedrohungserkennung für KI-Workloads
- Aktivierung des KI-Schutzes in Umgebungen mit mehreren Konten
- KI-Schutz für ein eigenständiges Konto aktivieren

So funktioniert der KI-Schutz

Wenn Sie den KI-Schutz für ein Konto oder für Ihr gesamtes Unternehmen aktivieren, beginnt GuardDuty automatisch mit der Erfassung von AWS CloudTrail Datenereignissen aus den KI-Diensten in den überwachten Konten. Sie müssen keinen Trail erstellen, die Protokollierung von Datenereignissen aktivieren oder Änderungen an Ihren KI-Anwendungen vornehmen.

Um die Datenereignisse zu erfassen, GuardDuty wird in jedem AWS CloudTrail überwachten Konto ein dienstbezogener Kanal erstellt. Der serviceverknüpfte Kanal streamt AWS CloudTrail Datenereignisse für Amazon Bedrock, Amazon Bedrock AgentCore und Amazon SageMaker AI sowie zugehörige KI-Ressourcen zur Analyse. GuardDuty Weil diesen GuardDuty Kanal erstellt und verwaltet:

- GuardDuty konfiguriert die Datenereigniseinstellungen des Kanals und der Kontoinhaber kann sie nicht ändern. Das bedeutet, dass die Erkennung von Bedrohungen nicht davon abhängt, dass der Kontoinhaber einen Trail konfiguriert oder verwaltet.
- Jedes überwachte Konto kann in der CloudTrail Konsole (unter Einstellungen, Service-linked Kanäle) oder durch Aufrufen der AWS CloudTrail ListChannels API-Operation bestätigen, dass der Kanal aktiv ist.

GuardDuty verwendet je nach Art des Ergebnisses zwei Erkennungsmethoden, um AI Protection-Ergebnisse zu generieren:

- GuardDuty Verwendet für die Typen Impact:IAMUser/AnomalousModelInvocation und Impact:IAMUser/CostHarvesting Auffinden ein Modell für maschinelles Lernen (ML) zur Erkennung von Anomalien, um die gesammelten Ereignisse zu analysieren und eine Grundlage für die normalen Modellaufrufaktivitäten für jede IAM-Identität zu erstellen und AWS-Konto GuardDuty generiert ein Ergebnis, wenn Aktivitäten erkannt werden, die erheblich von diesem Ausgangswert abweichen.
- GuardDutyGeneriert für den Impact:IAMUser/PromptInjection.Direct Ergebnistyp ein Ergebnis, wenn Amazon Bedrock Guardrails eine Aufforderung auswertet und auf der Grundlage des resultierenden Datenereignisses einen Prompt-Angriff erkennt. AWS CloudTrail

Weitere Informationen zu AWS CloudTrail Datenereignissen finden Sie im Benutzerhandbuch unter Protokollieren von Datenereignissen. AWS CloudTrail

Preisgestaltung für KI-Schutz

Wenn Sie den GuardDuty KI-Schutz aktivieren, GuardDuty fallen Gebühren für das Volumen der AWS CloudTrail analysierten Datenereignisse an, gemessen in GB. GuardDuty erstellt den mit dem Dienst verknüpften Kanal, ohne dass Ihnen CloudTrail zusätzliche Kosten entstehen. Die Kosten für die Erfassung dieser Datenereignisse sind in Ihren Nutzungskosten für AI Protection enthalten.

Außerdem fallen weiterhin Standardnutzungskosten für GuardDuty und alle anderen aktivierten Schutzpläne an. Aktuelle Preise und Beispiele finden Sie unter GuardDuty Amazon-Preise.

Zusätzliche Bedrohungserkennung für KI-Workloads

Zusätzlich zum AI Protection-Plan bieten die Amazon GuardDuty Foundational- und Lambda Protection-Pläne Erkennungen, mit denen Sie Bedrohungen für darauf aufbauende KI-Workloads schützen und erkennen können. AWS

Der GuardDuty Foundation-Plan überwacht AWS CloudTrail Verwaltungsereignisse, um verdächtige und böswillige Aktivitäten in KI-Workloads zu erkennen, die mithilfe von AWS Diensten wie Amazon Bedrock und Amazon AI erstellt wurden. SageMaker GuardDuty Kann beispielsweise Aktivitäten wie die folgenden identifizieren:

- Ungewöhnliches Entfernen der Amazon Bedrock-Sicherheitsleitplanken
- Eine Änderung an einer Datenquelle für das Modelltraining, die möglicherweise zu einem Datenvergiftungsangriff führen kann
- Die Protokollierung von Amazon Bedrock-Modellaufrufen, die auf Versuche hinweisen könnten, sich der Erkennung zu entziehen, wurde deaktiviert
- Ungewöhnliche Notebook-Instance oder Erstellung von Trainingsaufträgen in Amazon AI SageMaker
- Exfiltrierte Amazon Elastic Compute Cloud-Anmeldeinformationen, die möglicherweise zum Aufrufen von APIs in Amazon Bedrock, Amazon SageMaker AI oder selbstverwalteten KI-Workloads auf Amazon EC2-Instances, Amazon EKS-Clustern oder Amazon ECS-Aufgaben verwendet wurden.

GuardDuty Lambda Protection kann helfen, potenzielle Bedrohungen im Zusammenhang mit Amazon Bedrock-Agenten zu erkennen. Dazu können verdächtige Netzwerkaktivitäten wie Cryptomining und Kommunikation mit böswilligen Command-and-Control-Servern gehören. Diese Bedrohungen können durch einen Angriff auf die Lieferkette oder durch komplexe Aufforderungen verursacht werden.

Aktivierung des KI-Schutzes in Umgebungen mit mehreren Konten

In einer Umgebung mit mehreren Konten kann nur das delegierte GuardDuty Administratorkonto den KI-Schutz für die Mitgliedskonten in der Organisation aktivieren oder deaktivieren. Mitgliedskonten können diese Konfiguration nicht von ihren eigenen Konten aus ändern. Das delegierte GuardDuty

Administratorkonto verwaltet Mitgliedskonten mithilfe von und kann wählen AWS Organizations, ob der KI-Schutz für alle neuen Konten, die der Organisation beitreten, automatisch aktiviert werden soll. Weitere Informationen zu Umgebungen mit mehreren Konten finden Sie unter Verwaltung mehrerer Konten bei Amazon. GuardDuty

Aktivierung des KI-Schutzes für das delegierte Administratorkonto GuardDuty

Wählen Sie Ihre bevorzugte Zugriffsmethode, um AI Protection für das delegierte GuardDuty Administratorkonto zu aktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/
2. Wählen Sie im Navigationsbereich Protection Plans aus.
3. Wählen Sie Alle Aktivierungen konfigurieren aus. Unter AI Protection können Sie den aktuellen Konfigurationsstatus von AI Protection einsehen.
4. Führen Sie eine der folgenden Aktionen aus:

   Verwenden Für alle Konten aktivieren

   - Wählen Sie Für alle Konten aktivieren. Dadurch wird der Schutzplan für alle aktiven GuardDuty Konten in Ihrer AWS Organisation aktiviert, einschließlich der neuen Konten, die der Organisation beitreten.
   - Wählen Sie Speichern.

   Verwenden Konten manuell konfigurieren

   - Um den Schutzplan nur für das Konto des delegierten GuardDuty Administratorkontos zu aktivieren, wählen Sie Konten manuell konfigurieren.
   - Wählen Sie im Abschnitt Konto für delegierte GuardDuty Administratoren (dieses Konto) die Option Aktivieren aus.
   - Wählen Sie Speichern.

API/CLI

Führen Sie den API-Vorgang UpdateDetector aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den `features`-Objektnamen `name` als `AI_PROTECTION` und `status` als `ENABLED` oder `DISABLED` übergeben.

Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

Im folgenden Beispiel wird AI Protection für das delegierte GuardDuty Administratorkonto aktiviert. *`12abc34d567e8fa901bc2d34e56789f0`*Ersetzen Sie es durch die Detektor-ID Ihres Kontos und *`us-east-1`* durch die Region, in der Sie den KI-Schutz aktivieren möchten.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
region us-east-1 --features '[{"Name": "AI_PROTECTION", "Status": "ENABLED"}]'
```

Um den KI-Schutz zu deaktivieren, `ENABLED` ersetzen Sie ihn durch`DISABLED`.

Aktivierung des KI-Schutzes für alle vorhandenen aktiven Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um den KI-Schutz für alle vorhandenen aktiven Mitgliedskonten in der Organisation zu aktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Stellen Sie sicher, dass Sie die Anmeldedaten für das delegierte GuardDuty Administratorkonto verwenden.
2. Wählen Sie im Navigationsbereich die Option Protection Plans aus.
3. Wählen Sie Alle Aktivierungen konfigurieren aus. Wählen Sie unter KI-Schutz im Abschnitt Aktive Mitgliedskonten die Option Aktionen aus.
4. Wählen Sie im Dropdownmenü Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten.
5. Wählen Sie Speichern.

API/CLI

Um den KI-Schutz für Ihre Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren, führen Sie den UpdateMemberDetectors API-Vorgang mit Ihrem eigenen *detector ID* aus.

Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

Im folgenden Beispiel wird AI Protection für ein einzelnes Mitgliedskonto aktiviert. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`. Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --region us-east-1 --features '[{"Name":
 "AI_PROTECTION", "Status": "ENABLED"}]'
```

Wenn der Befehl erfolgreich ausgeführt wird, gibt er eine leere Liste von zurück`UnprocessedAccounts`. Wenn beim Ändern der Detektoreinstellungen für ein Konto Probleme auftreten, wird in der Antwort diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Auto-enable KI-Schutz für neue Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um den KI-Schutz für neue Konten zu aktivieren, die Ihrer Organisation beitreten.

In der Konsole kann das delegierte GuardDuty Administratorkonto AI Protection für neue Mitgliedskonten automatisch aktivieren, indem es entweder die Seite „Schutzpläne“ oder die Seite „Konten“ verwendet.

Console

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

   Stellen Sie sicher, dass Sie die Anmeldedaten für das delegierte GuardDuty Administratorkonto verwenden.
2. Führen Sie eine der folgenden Aktionen aus:
   - Verwenden Sie die Seite „Schutzpläne“:

1. Wählen Sie im Navigationsbereich die Option Schutzpläne aus.
2. Wählen Sie Alle Aktivierungen konfigurieren aus.
3. Wählen Sie unter KI-Schutz die Option Konten manuell konfigurieren aus und wählen Sie dann Automatisch für neue Mitgliedskonten aktivieren aus. Dieser Schritt stellt sicher, dass immer dann, wenn ein neues Konto Ihrer Organisation beitritt, der KI-Schutz für dieses Konto GuardDuty automatisch aktiviert wird. Nur das delegierte GuardDuty Administratorkonto der Organisation kann diese Konfiguration ändern.
4. Wählen Sie Speichern.

- Verwenden der Seite Konten:

1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
2. Wählen Sie auf der Seite Konten die Auto-enable Einstellungen aus.
3. Wählen Sie im Fenster „Einstellungen für automatische Aktivierung verwalten“ unter „KI-Schutz“ die Option „Für neue Konten aktivieren“ aus.
4. Wählen Sie Speichern.

API/CLI

Um den KI-Schutz für neue Mitgliedskonten zu aktivieren, führen Sie den UpdateOrganizationConfiguration API-Vorgang mit Ihrem eigenen *detector ID* aus.

Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

Das folgende Beispiel aktiviert den KI-Schutz für neue Konten, die Ihrer Organisation beitreten. Wenn Sie ihn nicht für alle neuen Konten aktivieren möchten, setzen Sie ihn `AutoEnable` auf`NONE`.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1 --auto-enable --features
 '[{"Name": "AI_PROTECTION", "AutoEnable": "NEW"}]'
```

KI-Schutz für ein eigenständiges Konto aktivieren

Ein eigenständiges Konto besitzt die Entscheidung, ob ein Schutzpaket für sein AWS Konto in einer bestimmten Region aktiviert oder deaktiviert werden soll.

Wenn Ihr Konto durch AWS Organizations oder auf Einladung mit einem GuardDuty Administratorkonto verknüpft ist, gilt dieser Abschnitt nicht für Sie. Informationen zur Verwaltung mehrerer Konten finden Sie unterAktivierung des KI-Schutzes in Umgebungen mit mehreren Konten.

Nachdem Sie den KI-Schutz aktiviert haben, GuardDuty beginnen Sie mit der Überwachung der Amazon Bedrock- und Amazon SageMaker AI-Modellaufrufaktivitäten, die CloudTrail für Ihr Konto erfasst werden.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um den KI-Schutz in Ihrem eigenständigen Konto zu aktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie in der Regionsauswahl in der oberen rechten Ecke eine Region aus, in der Sie den KI-Schutz aktivieren möchten.
3. Wählen Sie im Navigationsbereich Protection Plans aus.
4. Wählen Sie Alle Aktivierungen konfigurieren aus. Wählen Sie unter KI-Schutz die Option Aktivieren aus, um den KI-Schutz zu aktivieren.
5. Wählen Sie „Alle speichern“ und dann „Bestätigen und speichern“.

API/CLI

Führen Sie den UpdateDetector API-Vorgang mit Ihrer eigenen regionalen Detektor-ID aus und übergeben Sie das `features` Objekt `name` als `AI_PROTECTION` und `status` als`ENABLED`.

Alternativ können Sie den verwenden, AWS CLI um den KI-Schutz zu aktivieren. Führen Sie den folgenden Befehl aus und *`12abc34d567e8fa901bc2d34e56789f0`* ersetzen Sie ihn durch die Detektor-ID Ihres Kontos und *`us-east-1`* durch die Region, in der Sie den KI-Schutz aktivieren möchten.

Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
region us-east-1 --features '[{"Name": "AI_PROTECTION", "Status": "ENABLED"}]'
```

Um den KI-Schutz zu deaktivieren, `ENABLED` ersetzen Sie durch`DISABLED`.

GuardDuty EKS-Schutz

> **Note**
>
> Sie können EKS Protection zusammen mit allen anderen Schutzplänen von einer einzigen Seite in der GuardDuty Konsole aus konfigurieren. Weitere Informationen finden Sie unter Schutzpläne konfigurieren.

EKS Protection hilft Ihnen dabei, potenzielle Sicherheitsrisiken in Amazon Elastic Kubernetes Service (Amazon EKS) -Clustern in Ihrer AWS Umgebung zu erkennen. So können Sie beispielsweise erkennen, wenn ein nicht authentifizierter Akteur auf einen falsch konfigurierten EKS-Cluster zugreift, der versucht, geheime Daten oder AWS Anmeldeinformationen aus Ihrem Cluster zu sammeln. EKS Protection verwendet EKS-Auditprotokolle, um die Aktivitäten von Benutzern und Anwendungen zu analysieren.

Wenn Sie EKS Protection aktivieren, beginnt es GuardDuty automatisch mit der Überwachung Ihrer Amazon EKS-Cluster auf potenzielle Sicherheitsbedrohungen. GuardDuty verwendet einen eigenen unabhängigen Stream zum Sammeln und Analysieren Das EKS-Audit protokolliert in EKS Protection — es ist keine zusätzliche Konfiguration erforderlich.

Wenn auf der Grundlage der Überwachung des EKS-Auditprotokolls eine potenzielle Bedrohung GuardDuty erkannt wird, wird ein Sicherheitsergebnis generiert. Informationen zu den Erkennungstypen, die GuardDuty möglicherweise generiert werden, wenn Sie EKS Protection aktivieren, finden Sie unterArten der Suche nach EKS-Schutz.

> **Note**
>
> Um EKS-Auditprotokolle in Ihrem Konto anzuzeigen (optional), können Sie die Protokollierung der Amazon EKS-Kontrollebene so konfigurieren, dass CloudWatch Auditprotokolle an Logs gesendet werden. Diese Konfiguration ist unabhängig von EKS Protection und für die Sicherheitsüberwachungsfunktion in nicht erforderlich GuardDuty.

Kostenlose 30-Tage-Testversion

- Wenn Sie einen GuardDuty AWS-Konto in an AWS-Region zum ersten Mal aktivieren, erhalten Sie eine kostenlose 30-Tage-Testversion. In diesem Fall GuardDuty wird auch EKS Protection aktiviert, das in der kostenlosen 30-Tage-Testversion enthalten ist.
- Wenn Sie EKS Protection bereits verwenden GuardDuty und sich dafür entscheiden, es zum ersten Mal zu aktivieren, erhält Ihr Konto in dieser Region eine kostenlose 30-Tage-Testversion für EKS Protection.
- Sie können den EKS-Schutz in jeder Region jederzeit deaktivieren.
- Während der kostenlosen 30-Tage-Testversion erhalten Sie eine Schätzung Ihrer Nutzungskosten für dieses Konto und diese Region. Nach Ablauf der kostenlosen 30-Tage-Testversion wird EKS Protection GuardDuty nicht automatisch deaktiviert. Für Ihr Konto in dieser Region fallen ab sofort Nutzungskosten an. Weitere Informationen finden Sie unter Überwachung der Nutzung und Schätzung der Kosten.

Wenn Sie EKS Protection deaktivieren, wird die Überwachung und Analyse der EKS-Auditprotokolle für Ihre Amazon EKS-Ressourcen GuardDuty sofort beendet.

EKS-Schutz ist möglicherweise nicht überall verfügbar AWS-Regionen , wo er verfügbar GuardDuty ist. Weitere Informationen finden Sie unter Region-specific Verfügbarkeit von Funktionen.

> **Note**
>
> EKS Runtime Monitoring wird als Teil von Runtime Monitoring verwaltet. Weitere Informationen finden Sie unter GuardDuty Überwachung der Laufzeit.

Das EKS-Audit protokolliert in EKS Protection

EKS-Auditprotokolle erfassen sequentielle Aktionen innerhalb Ihres Amazon EKS-Clusters, einschließlich Aktivitäten von Benutzern, Anwendungen, die die Kubernetes-API verwenden, und der Kontrollebene. Die Prüfungs-Protokollierung ist eine Komponente aller Kubernetes-Cluster.

Weitere Informationen finden Sie unter Prüfung in der Kubernetes-Dokumentation.

Amazon EKS ermöglicht die Erfassung von EKS-Auditprotokollen als Amazon CloudWatch Logs über die Protokollierungsfunktion der EKS-Kontrollebene. GuardDuty verwaltet die Protokollierung Ihrer

Amazon EKS-Kontrollebene nicht und macht EKS-Auditprotokolle in Ihrem Konto nicht zugänglich, wenn Sie sie nicht für Amazon EKS aktiviert haben. Um den Zugriff auf und die Aufbewahrung Ihrer EKS-Auditprotokolle zu verwalten, müssen Sie die Protokollierungsfunktion der Amazon EKS-Kontrollebene konfigurieren. Weitere Informationen finden Sie unter Aktivieren und Deaktivieren von Protokollen auf Steuerebene im Amazon-EKS-Benutzerhandbuch.

EKS-Schutz in Umgebungen mit mehreren Konten aktivieren

In einer Umgebung mit mehreren Konten hat nur das delegierte GuardDuty Administratorkonto die Möglichkeit, die EKS-Schutzfunktion für die Mitgliedskonten in ihrer Organisation zu aktivieren oder zu deaktivieren. Die GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Das delegierte GuardDuty Administratorkonto verwaltet seine Mitgliedskonten mithilfe von AWS Organizations. Dieses delegierte GuardDuty Administratorkonto kann wählen, ob EKS-Schutz für alle neuen Konten automatisch aktiviert werden soll, wenn sie der Organisation beitreten. Weitere Informationen zu Umgebungen mit mehreren Konten finden Sie unter Verwaltung mehrerer Konten bei Amazon. GuardDuty

Konfiguration von EKS Audit Log Monitoring für ein delegiertes Administratorkonto GuardDuty

Wählen Sie Ihre bevorzugte Zugriffsmethode, um EKS Audit Log Monitoring für das delegierte GuardDuty Administratorkonto zu konfigurieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/
2. Wählen Sie im Navigationsbereich die Option Schutzpläne aus.
3. Wählen Sie Alle Aktivierungen konfigurieren aus. Unter EKS Audit Logs können Sie den aktuellen Konfigurationsstatus von EKS Audit Log Monitoring einsehen.
4. Führen Sie eine der folgenden Aktionen aus:

   Verwendung von Für alle Konten aktivieren

   - Wählen Sie Für alle Konten aktivieren. Dadurch wird der Schutzplan für alle aktiven GuardDuty Konten in Ihrer AWS Organisation aktiviert, einschließlich der neuen Konten, die der Organisation beitreten.
   - Wählen Sie Speichern.

Verwendung von Konten manuell konfigurieren

- Um den Schutzplan nur für das delegierte GuardDuty Administratorkonto zu aktivieren, wählen Sie Konten manuell konfigurieren.
- Wählen Sie im Abschnitt für das delegierte GuardDuty Administratorkonto (dieses Konto) die Option Aktivieren aus.
- Wählen Sie Speichern.

API/CLI

Führen Sie den API-Vorgang updateDetector aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den `features`-Objektnamen `name` als `EKS_AUDIT_LOGS` und `status` als `ENABLED` oder `DISABLED` übergeben.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

Sie können EKS Audit Log Monitoring aktivieren oder deaktivieren, indem Sie den folgenden AWS CLI Befehl ausführen. Stellen Sie sicher, dass Sie ein gültiges *`detector ID`* delegiertes GuardDuty Administratorkonto verwenden.

> **Note**
>
> Der folgende Beispielcode aktiviert EKS Audit Log Monitoring. Stellen Sie sicher, dass Sie es *`12abc34d567e8fa901bc2d34e56789f0`* durch das `detector-id` des delegierten GuardDuty Administratorkontos und *`555555555555`* durch das AWS-Konto des delegierten GuardDuty Administratorkontos ersetzen.

Das `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name": "EKS_AUDIT_LOGS", "Status": "ENABLED"}]'
```

Um EKS Audit Log Monitoring zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

Auto-enable EKS-Audit-Log-Überwachung für alle Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um EKS Audit Log Monitoring für alle vorhandenen aktiven Mitgliedskonten zu aktivieren.

Console

1. Melden Sie sich bei an AWS-Managementkonsole und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.
2. Führen Sie eine der folgenden Aktionen aus:

   Verwenden Sie die Seite „Schutzpläne“

   1. Wählen Sie im Navigationsbereich die Option Schutzpläne aus.
   2. Wählen Sie Alle Aktivierungen konfigurieren aus. Unter EKS Audit Logs können Sie den aktuellen Status von EKS Audit Log Monitoring für aktive Mitgliedskonten in Ihrer Organisation einsehen.
   3. Wählen Sie Für alle Konten aktivieren. Diese Aktion aktiviert EKS Audit Log Monitoring automatisch sowohl für die vorhandenen als auch für die neuen Konten in der Organisation.
   4. Wählen Sie Alle speichern und anschließend Bestätigen und speichern.

      > **Note**
      >
      > Die Aktualisierung der Konfiguration der Mitgliedskonten kann bis zu 24 Stunden dauern.

   Verwenden der Seite Konten

   1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
   2. Wählen Sie auf der Account-Seite Auto-enableEinstellungen und dann Accounts auf Einladung hinzufügen aus.

3. Wählen Sie im Fenster Einstellungen für automatische Aktivierung verwalten unter EKS Audit Log Monitoring die Option Für alle Konten aktivieren.
4. Wählen Sie Speichern.

Wenn Sie die Option Für alle Konten aktivieren nicht verwenden können und die Konfiguration von EKS Audit Log Monitoring für bestimmte Konten in Ihrer Organisation anpassen möchten, finden Sie weitere Informationen unter Aktivieren oder deaktivieren Sie EKS Audit Log Monitoring selektiv für Mitgliedskonten.

API/CLI

- Um EKS Audit Log Monitoring für Ihre Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren, führen Sie den updateMemberDetectorsAPI-Vorgang mit Ihrem eigenen *`detector ID`* aus.
- Das folgende Beispiel zeigt, wie Sie EKS Audit Log Monitoring für ein einzelnes Mitgliedskonto aktivieren können. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

  Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Einstellungsseite in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"name": "EKS_AUDIT_LOGS", "status": "ENABLED"}]'
```

  > **Note**
  >
  > Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Aktivierung von EKS Audit Log Monitoring für alle vorhandenen aktiven Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um EKS Audit Log Monitoring für alle vorhandenen aktiven Mitgliedskonten zu aktivieren.

Console

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Melden Sie sich mit den Anmeldeinformationen für das delegierte GuardDuty Administratorkonto an.
2. Wählen Sie im Navigationsbereich Schutzpläne aus.
3. Wählen Sie Alle Aktivierungen konfigurieren aus. Wählen Sie unter EKS Audit Logs im Abschnitt Aktive Mitgliedskonten die Option Aktionen aus.
4. Wählen Sie im Dropdownmenü Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten.
5. Wählen Sie Speichern.

API/CLI

- Um EKS Audit Log Monitoring für Ihre Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren, führen Sie den updateMemberDetectorsAPI-Vorgang mit Ihrem eigenen *`detector ID`* aus.
- Das folgende Beispiel zeigt, wie Sie EKS Audit Log Monitoring für ein einzelnes Mitgliedskonto aktivieren können. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

  Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Einstellungsseite in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"name": "EKS_AUDIT_LOGS", "status": "ENABLED"}]'
```

> **Note**
>
> Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Auto-enable EKS-Audit-Log-Überwachung für neue Mitgliedskonten

Die neu hinzugefügten Mitgliedskonten müssen aktiviert werden, GuardDuty bevor die Konfiguration des GuardDuty-initiated Malware-Scans ausgewählt werden kann. Die auf Einladung verwalteten Mitgliedskonten können den GuardDuty-initiated Malware-Scan für ihre Konten manuell konfigurieren. Weitere Informationen finden Sie unter Step 3 - Accept an invitation.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um EKS Audit Log Monitoring für neue Konten zu aktivieren, die Ihrer Organisation beitreten.

Console

Das delegierte GuardDuty Administratorkonto kann EKS Audit Log Monitoring für neue Mitgliedskonten in einer Organisation entweder über die Seite EKS Audit Log Monitoring oder Konten aktivieren.

So aktivieren Sie EKS Audit Log Monitoring automatisch für neue Mitgliedskonten

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

   Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.
2. Führen Sie eine der folgenden Aktionen aus:
   - Verwenden Sie die Seite „Schutzpläne“:

     1. Wählen Sie im Navigationsbereich die Option Schutzpläne aus.
     2. Wählen Sie Alle Aktivierungen konfigurieren aus. Konfigurieren Sie unter EKS Audit Logs die Einstellung für die automatische Aktivierung.

3. Wählen Sie Konten manuell konfigurieren.
4. Wählen Sie Automatisch für neue Mitgliedskonten aktivieren. Dieser Schritt stellt sicher, dass EKS Audit Log Monitoring bei jedem Beitritt eines neuen Kontos zu Ihrer Organisation automatisch für das Konto aktiviert wird. Nur das vom Unternehmen delegierte GuardDuty Administratorkonto kann diese Konfiguration ändern.
5. Wählen Sie Speichern.

- Verwenden der Seite Konten:

1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
2. Wählen Sie auf der Seite Konten die Option Auto-enableEinstellungen aus.
3. Wählen Sie im Fenster Einstellungen für automatische Aktivierung verwalten unter EKS Audit Log Monitoring die Option Für neue Konten aktivieren.
4. Wählen Sie Speichern.

API/CLI

- Um EKS Audit Log Monitoring für Ihre neuen Konten selektiv zu aktivieren oder zu deaktivieren, führen Sie den UpdateOrganizationConfigurationAPI-Vorgang mit Ihrem eigenen *`detector ID`* aus.
- Das folgende Beispiel zeigt, wie Sie EKS Audit Log Monitoring für die neuen Mitglieder aktivieren können, die Ihrer Organisation beitreten. Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

  Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Einstellungsseite in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
 "EKS_AUDIT_LOGS", "AutoEnable": "NEW"}]'
```

Aktivieren oder deaktivieren Sie EKS Audit Log Monitoring selektiv für Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um EKS Audit Log Monitoring für alle vorhandenen aktiven Mitgliedskonten zu aktivieren oder zu deaktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.

2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.

   Prüfen Sie auf der Seite Konten in der Spalte EKS Audit Log Monitoring den Status Ihres Mitgliedskontos.

3. So aktivieren oder deaktivieren Sie EKS Audit Log Monitoring

   Wählen Sie ein Konto aus, das Sie für EKS Audit Log Monitoring konfigurieren möchten. Sie können mehrere Konten gleichzeitig auswählen. Wählen Sie im Dropdown-Menü Schutzpläne bearbeiten die Option EKS Audit Log Monitoring und dann die entsprechende Option aus.

API/CLI

Um EKS Audit Log Monitoring für Ihre Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren, rufen Sie den updateMemberDetectorsAPI-Vorgang mit Ihrem eigenen auf. *`detector ID`*

Das folgende Beispiel zeigt, wie Sie EKS Audit Log Monitoring für ein einzelnes Mitgliedskonto aktivieren können. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`. Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Einstellungsseite in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --accountids 111122223333 --features '[{"Name": "EKS_AUDIT_LOGS", "Status":
 "ENABLED"}]'
```

EKS-Schutz für ein eigenständiges Konto aktivieren

Ein eigenständiges Konto hat die Entscheidung, einen Schutzplan für sein AWS Konto in einer bestimmten Region zu aktivieren oder zu deaktivieren.

Wenn Ihr Konto über oder über AWS Organizations die Einladungsmethode mit einem GuardDuty Administratorkonto verknüpft ist, gilt dieser Abschnitt nicht für Sie. Informationen zur Verwaltung mehrerer Konten finden Sie unterEKS-Schutz in Umgebungen mit mehreren Konten aktivieren.

Nachdem Sie EKS Protection aktiviert haben, GuardDuty beginnt es mit der Überwachung der EKS-Auditprotokolle für die Amazon EKS-Cluster in Ihrem Konto.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um EKS Protection in Ihrem eigenständigen Konto zu aktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie in der Regionsauswahl in der oberen rechten Ecke eine Region aus, in der Sie EKS Protection aktivieren möchten.
3. Wählen Sie im Navigationsbereich die Option Schutzpläne aus.
4. Wählen Sie Alle Aktivierungen konfigurieren aus. Wählen Sie unter EKS Audit Logs die Option Aktivieren aus, um EKS Protection zu aktivieren.
5. Wählen Sie Alle speichern und anschließend Bestätigen und speichern aus.

API/CLI

- Führen Sie den updateDetectorAPI-Vorgang mit der regionalen Detektor-ID des delegierten GuardDuty Administratorkontos aus und übergeben Sie den `features` Objektnamen `EKS_AUDIT_LOGS` und den Status als`ENABLED`.

  Alternativ können Sie EKS Protection auch aktivieren, indem Sie den AWS CLI Befehl a ausführen. Führen Sie den folgenden Befehl aus und *`12abc34d567e8fa901bc2d34e56789f0`* ersetzen Sie ihn durch die Melder-ID Ihres Kontos und *`us-east-1`* durch die Region, in der Sie EKS Protection aktivieren möchten.

  Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

  ```
  aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
  region us-east-1 --features [{"Name" : "EKS_AUDIT_LOGS", "Status" : "ENABLED"}]'
  ```

GuardDuty S3-Schutz

> **Note**
>
> Sie können S3 Protection zusammen mit allen anderen Schutzplänen von einer einzigen Seite in der GuardDuty Konsole aus konfigurieren. Weitere Informationen finden Sie unter Schutzpläne konfigurieren.

S3 Protection hilft Ihnen dabei, potenzielle Sicherheitsrisiken für Daten wie Datenexfiltration und -vernichtung in Ihren Amazon Simple Storage Service (Amazon S3) -Buckets zu erkennen. GuardDuty überwacht AWS CloudTrail Datenereignisse für Amazon S3, einschließlich API-Operationen auf Objektebene, um diese Risiken in allen Amazon S3 S3-Buckets in Ihrem Konto zu identifizieren.

Wenn auf der Grundlage der Überwachung von S3-Datenereignissen eine potenzielle Bedrohung GuardDuty erkannt wird, wird eine Sicherheitsfeststellung generiert. Informationen zu den Erkennungstypen, die bei der Aktivierung von S3 Protection generiert werden GuardDuty können, finden Sie unterGuardDuty S3 Schutzsuchtypen.

Standardmäßig umfasst die grundlegende Bedrohungserkennung die Überwachung AWS CloudTrail Verwaltungsereignisse zur Identifizierung potenzieller Bedrohungen in Ihren Amazon S3 S3-Ressourcen. Diese Datenquelle unterscheidet sich von den AWS CloudTrail Datenereignissen für S3, da beide unterschiedliche Arten von Aktivitäten in Ihrer Umgebung überwachen.

Sie können S3 Protection für ein Konto in jeder Region aktivieren, in der diese Funktion GuardDuty unterstützt wird. Auf diese Weise können Sie CloudTrail Datenereignisse für S3 in diesem Konto und dieser Region überwachen. Nachdem Sie S3 Protection aktiviert haben, können GuardDuty Sie Ihre Amazon S3 S3-Buckets vollständig überwachen und Ergebnisse für verdächtigen Zugriff auf die in Ihren S3-Buckets gespeicherten Daten generieren.

Um S3 Protection verwenden zu können, müssen Sie die S3-Datenereignisprotokollierung nicht explizit aktivieren oder konfigurieren. AWS CloudTrail

Kostenlose 30-Tage-Testversion

In der folgenden Liste wird erklärt, wie die kostenlose 30-Tage-Testversion für Ihr Konto funktionieren würde:

- Wenn Sie die Aktivierung GuardDuty AWS-Konto in einer neuen Region zum ersten Mal durchführen, erhalten Sie eine kostenlose 30-Tage-Testversion. In diesem Fall GuardDuty wird auch S3 Protection aktiviert, das in der kostenlosen Testversion enthalten ist.
- Wenn Sie S3 Protection bereits verwenden GuardDuty und sich entscheiden, es zum ersten Mal zu aktivieren, erhält Ihr Konto in dieser Region eine kostenlose 30-Tage-Testversion für S3 Protection.
- Sie können S3 Protection in jeder Region jederzeit deaktivieren.
- Während der kostenlosen 30-Tage-Testversion erhalten Sie eine Schätzung Ihrer Nutzungskosten für dieses Konto und diese Region. Nach Ablauf der kostenlosen 30-Tage-Testversion wird S3 Protection nicht automatisch deaktiviert. Für Ihr Konto in dieser Region fallen ab sofort Nutzungskosten an. Weitere Informationen finden Sie unter Überwachung der GuardDuty Nutzung und Schätzung der Kosten.

AWS CloudTrail Datenereignisse für S3

Datenereignisse, auch bekannt als Vorgänge auf der Datenebene, bieten Einblicke in die Ressourcen-Vorgänge, die für oder innerhalb einer Ressource ausgeführt wurden. Datenereignisse sind oft Aktivitäten mit hohem Volume.

Im Folgenden finden Sie Beispiele für CloudTrail Datenereignisse für S3, die überwacht GuardDuty werden können:

- `GetObject`-API-Operationen
- `PutObject`-API-Operationen
- `ListObjects`-API-Operationen
- `DeleteObject`-API-Operationen

Weitere Informationen zu diesen APIs finden Sie in der Amazon Simple Storage Service API-Referenz.

Wie GuardDuty werden CloudTrail Datenereignisse für S3 verwendet

Wenn Sie S3 Protection aktivieren, GuardDuty beginnt es mit der Analyse von CloudTrail Datenereignissen für S3 aus all Ihren S3-Buckets und überwacht sie auf böswillige und verdächtige Aktivitäten. Weitere Informationen finden Sie unter AWS CloudTrail Verwaltungsereignisse.

Wenn ein nicht authentifizierter Benutzer auf ein S3-Objekt zugreift, bedeutet dies, dass das S3-Objekt öffentlich zugänglich ist. Verarbeitet solche Anfragen daher GuardDuty nicht. GuardDuty verarbeitet die an die S3-Objekte gestellten Anfragen unter Verwendung gültiger IAM (AWS Identity and Access Management) - oder AWS STS (AWS -Security-Token-Service) -Anmeldeinformationen.

> **Hinweis**
>
> GuardDuty Überwacht nach der Aktivierung von S3 Protection die Datenereignisse aus den Amazon S3 S3-Buckets, die sich in derselben Region befinden, in der Sie die Aktivierung aktiviert haben. GuardDuty

Wenn Sie den S3-Schutz in Ihrem Konto in einer bestimmten Region deaktivieren, wird die S3-Datenereignisüberwachung der in Ihren S3-Buckets gespeicherten Daten GuardDuty beendet. GuardDuty generiert für Ihr Konto in dieser Region keine S3-Protection-Suchtypen mehr.

GuardDuty Verwendung von CloudTrail Datenereignissen für S3 für Angriffssequenzen

GuardDuty Erweiterte Bedrohungserkennungerkennt mehrstufige Angriffssequenzen, die grundlegende Datenquellen, AWS Ressourcen und Zeitpläne in einem Konto umfassen. Wenn eine Abfolge von Ereignissen GuardDuty beobachtet wird, die auf eine kürzliche oder laufende verdächtige Aktivität in Ihrem Konto hindeuten, GuardDuty generiert das System eine entsprechende Erkennung der Angriffssequenz.

Wenn Sie Extended Threat Detection aktivieren GuardDuty, wird die erweiterte Bedrohungserkennung standardmäßig auch in Ihrem Konto aktiviert. Diese Funktion deckt das Bedrohungsszenario im Zusammenhang mit CloudTrail Verwaltungsereignissen ohne zusätzliche Kosten ab. Um Extended Threat Detection jedoch in vollem Umfang nutzen zu können, GuardDuty empfiehlt es sich, S3 Protection zu aktivieren, um Bedrohungsszenarien im Zusammenhang mit CloudTrail Datenereignissen für S3 abzudecken.

Nachdem Sie S3 Protection aktiviert haben, deckt GuardDuty es automatisch die Bedrohungsszenarien der Angriffssequenz ab, z. B. die Kompromittierung oder Zerstörung von Daten, bei denen Ihre Amazon S3 S3-Ressourcen betroffen sein könnten.

S3-Schutz in Umgebungen mit mehreren Konten aktivieren

In einer Umgebung mit mehreren Konten hat nur das delegierte GuardDuty Administratorkonto die Möglichkeit, den S3-Schutz für die Mitgliedskonten in seiner Organisation zu konfigurieren (zu aktivieren oder zu deaktivieren). AWS Die GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Das delegierte GuardDuty Administratorkonto verwaltet seine Mitgliedskonten mithilfe von AWS Organizations. Das delegierte GuardDuty Administratorkonto kann wählen, ob S3 Protection automatisch für alle Konten, nur für neue Konten oder für keine Konten in der Organisation aktiviert werden soll. Weitere Informationen finden Sie unter Verwalten von Konten mit AWS Organizations.

S3-Schutz für das delegierte Administratorkonto GuardDuty aktivieren

Wählen Sie Ihre bevorzugte Zugriffsmethode, um S3 Protection für das delegierte GuardDuty Administratorkonto zu aktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/
2. Wählen Sie im Navigationsbereich S3 Protection.
3. Wählen Sie auf der Seite S3 Protection die Option Bearbeiten.
4. Führen Sie eine der folgenden Aktionen aus:

   Verwendung von Für alle Konten aktivieren

   - Wählen Sie Für alle Konten aktivieren. Dadurch wird der Schutzplan für alle aktiven GuardDuty Konten in Ihrer AWS Organisation aktiviert, einschließlich der neuen Konten, die der Organisation beitreten.
   - Wählen Sie Speichern.

   Verwendung von Konten manuell konfigurieren

   - Um den Schutzplan nur für das delegierte GuardDuty Administratorkonto zu aktivieren, wählen Sie Konten manuell konfigurieren.
   - Wählen Sie im Abschnitt für das delegierte GuardDuty Administratorkonto (dieses Konto) die Option Aktivieren aus.
   - Wählen Sie Speichern.

API/CLI

Verwenden Sie für die Ausführung updateDetectordie Detektor-ID des delegierten GuardDuty Administratorkontos für die aktuelle Region und übergeben Sie das `features` Objekt `name` als `S3_DATA_EVENTS` und `status` als. `ENABLED`

Alternativ können Sie S3 Protection konfigurieren, indem Sie AWS Command Line Interface Führen Sie den folgenden Befehl aus und achten Sie darauf, ihn *`12abc34d567e8fa901bc2d34e56789f0`* durch die Detektor-ID des delegierten GuardDuty Administratorkontos für die aktuelle Region zu ersetzen.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name": "S3_DATA_EVENTS", "Status": "ENABLED"}]'
```

Auto-enable S3-Schutz für alle Mitgliedskonten in der Organisation

Wählen Sie Ihre bevorzugte Zugriffsmethode, um S3 Protection für das delegierte GuardDuty Administratorkonto zu aktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

   Melden Sie sich mit Ihrem Administratorkonto an.
2. Führen Sie eine der folgenden Aktionen aus:

   Verwenden der Seite S3 Protection

   1. Wählen Sie im Navigationsbereich S3 Protection.
   2. Wählen Sie Für alle Konten aktivieren. Diese Aktion aktiviert automatisch S3 Protection sowohl für bestehende als auch für neue Konten in der Organisation.
   3. Wählen Sie Speichern.

> **Note**
>
> Die Aktualisierung der Konfiguration der Mitgliedskonten kann bis zu 24 Stunden dauern.

Verwenden der Seite Konten

1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
2. Wählen Sie auf der Seite Konten die Auto-enableEinstellungen vor Konten auf Einladung hinzufügen aus.
3. Wählen Sie im Fenster Einstellungen für automatische Aktivierung verwalten die Option Für alle Konten aktivieren unter S3 Protection.
4. Wählen Sie Speichern.

Falls Sie die Option Für alle Konten aktivieren nicht verwenden können, finden Sie weitere Informationen unter Aktivieren Sie S3 Protection selektiv in Mitgliedskonten.

API/CLI

- Um S3 Protection selektiv für Ihre Mitgliedskonten zu aktivieren, rufen Sie den updateMemberDetectorsAPI-Vorgang mit Ihrem eigenen auf. *`detector ID`*
- Das folgende Beispiel zeigt, wie Sie S3 Protection für ein einzelnes Mitgliedskonto aktivieren können. Stellen Sie sicher, dass Sie es *`12abc34d567e8fa901bc2d34e56789f0`* durch das `detector-id` des delegierten GuardDuty Administratorkontos ersetzen, und. *`111122223333`*

  Das `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"name": "S3_DATA_EVENTS", "status": "ENABLED"}]'
```

> **Note**
>
> Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Aktivieren Sie S3 Protection für alle vorhandenen aktiven Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um S3 Protection für alle vorhandenen aktiven Mitgliedskonten in Ihrer Organisation zu aktivieren.

Console

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Melden Sie sich mit den Anmeldeinformationen für das delegierte GuardDuty Administratorkonto an.
2. Wählen Sie im Navigationsbereich S3 Protection.
3. Auf der Seite S3 Protection können Sie den aktuellen Status der Konfiguration anzeigen. Wählen Sie im Abschnitt Aktive Mitgliedskonten die Option Aktionen.
4. Wählen Sie im Dropdownmenü Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten.
5. Wählen Sie Bestätigen aus.

API/CLI

- Um S3 Protection selektiv für Ihre Mitgliedskonten zu aktivieren, rufen Sie den updateMemberDetectorsAPI-Vorgang mit Ihrem eigenen auf. *`detector ID`*
- Das folgende Beispiel zeigt, wie Sie S3 Protection für ein einzelnes Mitgliedskonto aktivieren können. Stellen Sie sicher, dass Sie es *`12abc34d567e8fa901bc2d34e56789f0`* durch das `detector-id` des delegierten GuardDuty Administratorkontos ersetzen, und. *`111122223333`*

Das `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"name": "S3_DATA_EVENTS", "status": "ENABLED"}]'
```

> **Note**
>
> Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Auto-enable S3-Schutz für neue Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um S3 Protection für neue Konten, die Ihrer Organisation beitreten, zu aktivieren.

Console

Das delegierte GuardDuty Administratorkonto kann über die Konsole entweder über die Seite S3-Schutz oder Konten für neue Mitgliedskonten in einer Organisation aktiviert werden.

So richten Sie Automatisches Aktivieren von S3 Protection für neue Mitgliedskonten ein

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

   Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.
2. Führen Sie eine der folgenden Aktionen aus:
   - Verwendung der Seite S3 Protection:

     1. Wählen Sie im Navigationsbereich S3 Protection.

2. Wählen Sie auf der Seite S3 Protection die Option Bearbeiten.
3. Wählen Sie Konten manuell konfigurieren.
4. Wählen Sie Automatisch für neue Mitgliedskonten aktivieren. Dieser Schritt stellt sicher, dass S3 Protection jedes mal automatisch für das Konto aktiviert wird, wenn ein neues Konto Ihrer Organisation beitritt. Nur das delegierte GuardDuty Administratorkonto der Organisation kann diese Konfiguration ändern.
5. Wählen Sie Speichern.

- Verwenden der Seite Konten:

1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
2. Wählen Sie auf der Seite Konten die Option Auto-enableEinstellungen aus.
3. Wählen Sie im Fenster Einstellungen für automatische Aktivierung verwalten unter S3 Protection die Option Für neue Konten aktivieren.
4. Wählen Sie Speichern.

API/CLI

- Um S3 Protection selektiv für Ihre Mitgliedskonten zu aktivieren, rufen Sie den UpdateOrganizationConfigurationAPI-Vorgang mit Ihrem eigenen auf. *detector ID*
- Das folgende Beispiel zeigt, wie Sie S3 Protection für ein einzelnes Mitgliedskonto aktivieren können. Legen Sie die Einstellungen so fest, dass der Schutzplan in dieser Region für neue Konten (`NEW`), die der Organisation beitreten, für alle Konten (`ALL`) oder für keines der Konten (`NONE`) in der Organisation automatisch aktiviert oder deaktiviert wird. Weitere Informationen finden Sie unter Auto EnableOrganizationMembers. Je nach Ihren Einstellungen müssen Sie möglicherweise `NEW` durch `ALL` oder `NONE` ersetzen.

  Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
 "S3_DATA_EVENTS", "autoEnable": "NEW"}]'
```

- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto

Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Aktivieren Sie S3 Protection selektiv in Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um S3 Protection selektiv für Mitgliedskonten zu aktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

   Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.
2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.

   Auf der Seite Konten finden Sie in der Spalte S3 Protection den Status Ihres Mitgliedskontos.
3. Um S3 Protection selektiv zu aktivieren

   Wählen Sie das Konto aus, für das Sie S3 Protection aktivieren möchten. Sie können mehrere Konten gleichzeitig auswählen. Wählen Sie im Dropdown-Menü Schutzpläne bearbeiten die Option S3Pro aus und wählen Sie dann die entsprechende Option aus.

API/CLI

Um S3 Protection selektiv für Ihre Mitgliedskonten zu aktivieren, führen Sie den updateMemberDetectorsAPI-Vorgang mit Ihrer eigenen Detektor-ID aus. Das folgende Beispiel zeigt, wie Sie S3 Protection für ein einzelnes Mitgliedskonto aktivieren können. Um die Funktion zu deaktivieren, ersetzen Sie `true` durch `false`.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

```
 aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 123456789012 --features
 '[{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"}]'
```

> **Note**
>
> Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

> **Note**
>
> Wenn Sie Skripts verwenden, um neue Konten zu integrieren und S3 Protection in Ihren neuen Konten deaktivieren möchten, können Sie den API-Vorgang createDetectormit dem optionalen `dataSources`-Objekt ändern, wie in diesem Thema beschrieben.

S3-Schutz für ein eigenständiges Konto aktivieren

Ein eigenständiges Konto hat die Entscheidung, einen Schutzplan AWS-Konto in einem bestimmten Bereich zu aktivieren oder zu deaktivieren AWS-Region.

Wenn Ihr Konto über oder über AWS Organizations die Einladungsmethode mit einem GuardDuty Administratorkonto verknüpft ist, gilt dieser Abschnitt nicht für Ihr Konto. Weitere Informationen finden Sie unter S3-Schutz in Umgebungen mit mehreren Konten aktivieren.

Nachdem Sie S3 Protection aktiviert haben, GuardDuty beginnt es mit der Überwachung von AWS CloudTrail Datenereignissen für die S3-Buckets in Ihrem Konto.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um S3 Protection für ein einzelnes Konto zu konfigurieren.

Console

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie in der Regionsauswahl in der oberen rechten Ecke eine Region aus, in der Sie S3 Protection aktivieren möchten.

3. Wählen Sie im Navigationsbereich S3 Protection.
4. Auf der Seite S3 Protection finden Sie den aktuellen Status von S3 Protection für Ihr Konto. Wählen Sie Aktivieren oder Deaktivieren, um S3 Protection zu einem beliebigen Zeitpunkt zu aktivieren oder zu deaktivieren.
5. Wählen Sie Bestätigen, um Ihre Auswahl zu bestätigen.

API/CLI

Führen Sie updateDetectorden Vorgang aus, indem Sie Ihre gültige Melder-ID für die aktuelle Region verwenden und das `features` Objekt entsprechend den `name` Einstellungen `S3_DATA_EVENTS` übergeben, `ENABLED` um den S3-Schutz zu aktivieren.

> **Note**
>
> Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

Alternativ können Sie verwenden AWS Command Line Interface. Um S3 Protection zu aktivieren, führen Sie den folgenden Befehl aus und *12abc34d567e8fa901bc2d34e56789f0* ersetzen Sie ihn durch die Melder-ID Ihres Kontos und *us-east-1* durch die Region, in der Sie S3 Protection aktivieren möchten.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
region us-east-1 --features '[{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"}]'
```

GuardDuty Überwachung der Laufzeit

> **Note**
>
> Sie können Runtime Monitoring zusammen mit allen anderen Schutzplänen von einer einzigen Seite in der GuardDuty Konsole aus konfigurieren. Weitere Informationen finden Sie unter Schutzpläne konfigurieren.

Runtime Monitoring beobachtet und analysiert Ereignisse auf Betriebssystemebene, Netzwerk- und Dateiereignisse, um Ihnen zu helfen, potenzielle Bedrohungen in bestimmten AWS Workloads in Ihrer Umgebung zu erkennen.

Unterstützte AWS Ressourcen in Runtime Monitoring — Runtime Monitoring deckt die Bedrohungserkennung für Ressourcen von Amazon Elastic Kubernetes Service (Amazon EKS), Amazon Elastic Container Service (Amazon ECS) on AWS Fargate und Amazon Elastic Compute Cloud (Amazon EC2) ab.

GuardDuty unterstützt keine Amazon EKS-Cluster, die auf laufen. AWS Fargate

In diesem Dokument und anderen Abschnitten, die sich auf Runtime Monitoring beziehen, wird die Terminologie des Ressourcentyps GuardDuty verwendet, um auf Amazon EKS-, Fargate-, Amazon ECS- und Amazon EC2-Ressourcen zu verweisen.

Runtime Monitoring verwendet einen GuardDuty Sicherheitsagenten, der Einblick in das Laufzeitverhalten wie Dateizugriff, Prozessausführung, Befehlszeilenargumente und Netzwerkverbindungen bietet. Für jeden Ressourcentyp, den Sie auf potenzielle Bedrohungen überwachen möchten, können Sie den Security Agent für diesen bestimmten Ressourcentyp entweder automatisch oder manuell verwalten (mit Ausnahme von Fargate (nur Amazon ECS)). Die automatische Verwaltung des Security Agents bedeutet, dass Sie GuardDuty gestatten, den Security Agent in Ihrem Namen zu installieren und zu aktualisieren. Wenn Sie den Security Agent für Ihre Ressourcen jedoch manuell verwalten, sind Sie dafür verantwortlich, den Security Agent bei Bedarf zu installieren und zu aktualisieren.

Mit dieser erweiterten Funktion GuardDuty können Sie potenzielle Bedrohungen identifizieren und darauf reagieren, die auf Anwendungen und Daten abzielen, die in Ihren einzelnen Workloads und Instances ausgeführt werden. Eine Bedrohung kann beispielsweise dadurch entstehen, dass

ein einzelner Container kompromittiert wird, auf dem eine anfällige Web-Anwendung ausgeführt wird. Diese Web-Anwendung verfügt möglicherweise über Zugriffsberechtigungen für die zugrunde liegenden Container und Workloads. In diesem Fall könnten falsch konfigurierte Anmeldedaten möglicherweise zu einem umfassenderen Zugriff auf das Konto und die darin gespeicherten Daten führen.

Durch die Analyse der Laufzeitereignisse der einzelnen Container und Workloads GuardDuty können Sie in einer ersten Phase potenzielle Gefährdungen eines Containers und der zugehörigen AWS Anmeldeinformationen erkennen und Versuche, Rechte zu erweitern, verdächtige API-Anfragen und böswillige Zugriffe auf die Daten in Ihrer Umgebung erkennen.

Inhalt

- Funktionsweise
- Wie funktioniert die kostenlose 30-Tage-Testversion in Runtime Monitoring
- Voraussetzungen für die Aktivierung von Runtime Monitoring
- Laufzeitüberwachung aktivieren GuardDuty
- Verwaltung der GuardDuty Sicherheitsagenten
- Überprüfung der Statistiken zur Laufzeitabdeckung und Behebung von Problemen
- Einrichten der CPU- und Arbeitsspeicherüberwachung
- Verwenden von gemeinsam genutzter VPC mit Runtime Monitoring
- Verwendung von Infrastructure as Code (IaC) mit GuardDuty automatisierten Sicherheitsagenten
- Gesammelte Runtime-Ereignistypen, die GuardDuty verwendet
- Amazon ECR-Repository-Hosting-Agent GuardDuty
- Zwei Security Agents auf demselben zugrunde liegenden Host
- EKS-Laufzeitüberwachung in GuardDuty
- GuardDuty Release-Versionen des Security Agents
- Deaktivieren, Deinstallieren und Bereinigen von Ressourcen in Runtime Monitoring

Funktionsweise

Um Runtime Monitoring verwenden zu können, müssen Sie Runtime Monitoring aktivieren und dann den GuardDuty Security Agent verwalten. In der folgenden Liste wird dieser zweistufige Prozess erklärt:

1. Aktivieren Sie Runtime Monitoring für Ihr Konto, damit es die Laufzeitereignisse akzeptieren GuardDuty kann, die es von Ihren Amazon EC2-Instances, Amazon ECS-Clustern und Amazon EKS-Workloads empfängt.
2. Verwalten Sie den GuardDuty Agenten für die einzelnen Ressourcen, für die Sie das Laufzeitverhalten überwachen möchten. Je nach Ressourcentyp können Sie wählen zwischen:
   - Verwenden Sie die automatische Agentenkonfiguration, bei der die Agentenbereitstellung GuardDuty verwaltet und automatisch ein Amazon Virtual Private Cloud (Amazon VPC) - Endpunkt erstellt wird.
   - Installieren Sie den Agenten manuell. Dazu müssen Sie den VPC-Endpunkt als Voraussetzung erstellen.

   Der Security Agent verwendet einen VPC-Endpunkt, um Ereignisse an diese weiterzuleiten GuardDuty und so sicherzustellen, dass die Daten im Netzwerk bleiben. AWS Dieser Ansatz erhöht die Sicherheit und ermöglicht GuardDuty die Überwachung und Analyse des Laufzeitverhaltens Ihrer Ressourcen (Amazon EKS, Amazon EC2 und AWS Fargate-Amazon ECS). GuardDuty verwendet Instance-Identitätsrollen, die den Security Agent für jeden Ressourcentyp authentifizieren, um die zugehörigen Laufzeitereignisse an den VPC-Endpunkt zu senden.

> **Note**
>
> GuardDuty analysiert Laufzeitereignisse in Ihrer AWS Umgebung, verwendet sie intern zur Bedrohungserkennung und präsentiert die Ergebnisse in Form von Ergebnissen.

Wenn Sie den Security Agent (entweder manuell oder über GuardDuty) in EKS Runtime Monitoring oder Runtime Monitoring für EC2-Instances verwalten und derzeit auf einer Amazon EC2-Instance bereitgestellt GuardDuty wird und ihn Gesammelte Laufzeit-Ereignistypen von dieser Instance erhält, GuardDuty wird Ihnen die Analyse der VPC-Flow-Logs aus dieser Amazon EC2-Instance nicht in Rechnung gestellt. AWS-Konto Dies hilft, doppelte Nutzungskosten für das Konto GuardDuty zu vermeiden.

In den folgenden Themen wird erläutert, wie die Aktivierung von Runtime Monitoring und die Verwaltung des GuardDuty Security Agents für jeden Ressourcentyp unterschiedlich funktionieren.

Inhalt

- Funktionsweise von Runtime Monitoring mit Amazon-EKS-Clustern

- So funktioniert Runtime Monitoring mit Amazon EC2-Instances
- So funktioniert Runtime Monitoring mit Fargate (nur Amazon ECS)
- Nachdem Sie Runtime Monitoring aktiviert haben

Funktionsweise von Runtime Monitoring mit Amazon-EKS-Clustern

Runtime Monitoring verwendet ein EKS-Add-on `aws-guardduty-agent`, das auch als GuardDuty Security Agent bekannt ist. Nachdem der GuardDuty Security Agent auf Ihren EKS-Clustern bereitgestellt wurde, GuardDuty kann er Laufzeitereignisse für diese EKS-Cluster empfangen.

> **Hinweise**
>
> Runtime Monitoring unterstützt Amazon EKS-Cluster, die auf Amazon EC2-Instances und Amazon EKS Auto Mode ausgeführt werden.
> Runtime Monitoring unterstützt keine Amazon EKS-Cluster mit Amazon EKS-Hybridknoten und solche, die darauf AWS Fargate laufen.
> Informationen zu diesen Amazon EKS-Funktionen finden Sie unter Was ist Amazon EKS? im Amazon EKS-Benutzerhandbuch .

Sie können die Laufzeitereignisse Ihrer Amazon EKS-Cluster entweder auf Konto- oder Clusterebene überwachen. Sie können den GuardDuty Security Agent nur für die Amazon EKS-Cluster verwalten, die Sie im Hinblick auf die Erkennung von Bedrohungen überwachen möchten. Sie können den GuardDuty Security Agent entweder manuell verwalten oder indem GuardDuty Sie die automatische Agentenkonfiguration verwenden, indem Sie ihm die Verwaltung in Ihrem Namen gestatten.

Wenn Sie den Ansatz der automatisierten Agentenkonfiguration verwenden, GuardDuty um die Bereitstellung des Security Agents in Ihrem Namen zu verwalten, wird automatisch ein Amazon Virtual Private Cloud (Amazon VPC) -Endpunkt erstellt. Der Security Agent übermittelt die Laufzeitereignisse GuardDuty mithilfe dieses Amazon VPC-Endpunkts an.

Erstellt zusammen mit dem VPC-Endpunkt GuardDuty auch eine neue Sicherheitsgruppe. Die Regeln für eingehenden Verkehr (Eingangsregeln) steuern den Datenverkehr, der die Ressourcen erreichen darf, die der Sicherheitsgruppe zugeordnet sind. GuardDuty fügt Regeln für eingehenden Verkehr hinzu, die dem VPC-CIDR-Bereich für Ihre Ressource entsprechen, und passt sich diesen an, wenn sich der CIDR-Bereich ändert. Weitere Informationen finden Sie unter VPC-CIDR-Bereich im Amazon VPC-Benutzerhandbuch.

Hinweise

- Für die Nutzung des VPC-Endpunkts fallen keine zusätzlichen Kosten an.
- Arbeiten mit zentralisierter VPC mit automatisiertem Agenten — Wenn Sie die GuardDuty automatische Agentenkonfiguration für einen Ressourcentyp verwenden, GuardDuty wird in Ihrem Namen ein VPC-Endpunkt für alle VPCs erstellt. Dazu gehören die zentralisierte VPC und die Spoke-VPCs. GuardDuty unterstützt nicht die Erstellung eines VPC-Endpunkts nur für die zentralisierte VPC. Weitere Informationen zur Funktionsweise der zentralisierten VPC finden Sie unter Interface VPC Endpoints im AWS Whitepaper — Aufbau einer skalierbaren und sicheren Netzwerkinfrastruktur. Multi-VPC AWS

Ansätze zur Verwaltung von GuardDuty Sicherheitsagenten in Amazon EKS-Clustern

Vor dem 13. September 2023 konnten Sie die Verwaltung des Security Agents auf Kontoebene konfigurieren GuardDuty . Dieses Verhalten deutete darauf hin, dass der Security Agent standardmäßig auf allen EKS-Clustern GuardDuty verwaltet wird, die zu einem gehören AWS-Konto. GuardDuty Bietet jetzt eine granulare Funktion, mit der Sie die EKS-Cluster auswählen können, in denen Sie den Security Agent verwalten GuardDuty möchten.

Wenn Sie Den GuardDuty Security Agent manuell verwalten wählen, können Sie immer noch die EKS-Cluster auswählen, die Sie überwachen möchten. Um den Agenten jedoch manuell zu verwalten, ist die Erstellung eines Amazon VPC-Endpunkts für Sie eine AWS-Konto Voraussetzung.

Note

Unabhängig davon, welchen Ansatz Sie zur Verwaltung des GuardDuty Security Agents verwenden, ist EKS Runtime Monitoring immer auf Kontoebene aktiviert.

Themen

- Verwalten Sie den Security Agent über GuardDuty
- Den GuardDuty Security Agent manuell verwalten

Verwalten Sie den Security Agent über GuardDuty

GuardDuty setzt den Security Agent in Ihrem Namen ein und verwaltet ihn. Sie können die EKS-Cluster in Ihrem Konto jederzeit überwachen, indem Sie einen der folgenden Ansätzen verwenden.

Themen

- Überwachen Sie alle EKS-Cluster
- Selektive EKS-Cluster ausschließen
- Schließen Sie selektive EKS-Cluster ein

Überwachen Sie alle EKS-Cluster

Verwenden Sie diesen Ansatz, wenn Sie GuardDuty den Security Agent für alle EKS-Cluster in Ihrem Konto bereitstellen und verwalten möchten. Standardmäßig GuardDuty wird der Security Agent auch auf einem potenziell neuen EKS-Cluster bereitgestellt, der in Ihrem Konto erstellt wurde.

Auswirkungen der Verwendung dieses Ansatzes

- GuardDuty erstellt einen Amazon Virtual Private Cloud (Amazon VPC) -Endpunkt, über den der GuardDuty Security Agent die Laufzeitereignisse übermittelt GuardDuty. Bei der Verwaltung des Security Agents fallen keine zusätzlichen Kosten für die Erstellung des Amazon VPC-Endpunkts an. GuardDuty
- Es ist erforderlich, dass Ihr Worker-Knoten über einen gültigen Netzwerkpfad zu einem aktiven `guardduty-data` VPC-Endpunkt verfügt. GuardDuty stellt den Security Agent auf Ihren EKS-Clustern bereit. Amazon Elastic Kubernetes Service (Amazon EKS) koordiniert die Bereitstellung des Sicherheitsagenten auf den Knoten innerhalb der EKS-Cluster.
- GuardDuty Wählt auf der Grundlage der IP-Verfügbarkeit das Subnetz aus, um einen VPC-Endpunkt zu erstellen. Wenn Sie erweiterte Netzwerktopologien verwenden, müssen Sie überprüfen, ob die Konnektivität möglich ist.

Selektive EKS-Cluster ausschließen

Verwenden Sie diesen Ansatz, wenn Sie GuardDuty den Security Agent für alle EKS-Cluster in Ihrem Konto verwalten, aber ausgewählte EKS-Cluster ausschließen möchten. Bei dieser Methode wird ein Tag-basierter [1] Ansatz verwendet, bei dem Sie die EKS-Cluster taggen können, für die Sie keine Laufzeit-Ereignisse erhalten möchten. Das vordefinierte Tag muss`GuardDutyManaged: false` als Schlüssel-Wert-Paar haben.

Auswirkungen der Verwendung dieses Ansatzes

Bei diesem Ansatz müssen Sie die automatische GuardDuty Agentenverwaltung erst aktivieren, nachdem Sie den EKS-Clustern, die Sie von der Überwachung ausschließen möchten, Tags hinzugefügt haben.

Daher gilt auch für diesen Ansatz die Auswirkung von Verwalten Sie den Security Agent über GuardDuty. Wenn Sie Tags hinzufügen, bevor Sie die automatische GuardDuty Agentenverwaltung aktivieren, GuardDuty wird der Security Agent für die EKS-Cluster, die von der Überwachung ausgeschlossen sind, weder bereitgestellt noch verwaltet.

Überlegungen

- Sie müssen das Tag-Schlüssel-Wert-Paar wie folgt hinzufügen`GuardDutyManaged: false` für die ausgewählten EKS-Cluster, bevor Sie die automatische Agentenkonfiguration aktivieren. Andernfalls wird der GuardDuty Security Agent auf allen EKS-Clustern bereitgestellt, bis Sie das Tag verwenden.
- Sie müssen verhindern, dass die Tags geändert werden, es sei denn, es handelt sich um vertrauenswürdige Identitäten.

  > **Important**
  >
  > Verwalten Sie die Berechtigungen zum Ändern des Werts des `GuardDutyManaged`-Tags für Ihren EKS-Cluster mithilfe von Service-Kontrollrichtlinie oder IAM-Richtlinien. Weitere Informationen finden Sie unter Service-Kontrollrichtlinien (SCPs) im Benutzerhandbuch für AWS Organizations oder Zugriff auf AWS -Ressourcen steuern im IAM-Benutzerhandbuch.

- Bei einem potenziell neuen EKS-Cluster, den Sie nicht überwachen möchten, stellen Sie sicher, dass Sie zum Zeitpunkt der Erstellung dieses EKS-Clusters das `false` Schlüssel-Wert-Paar`GuardDutyManaged:` hinzufügen.
- Bei diesem Ansatz werden auch dieselben Überlegungen berücksichtigt, wie für Überwachen Sie alle EKS-Cluster angegeben.

Schließen Sie selektive EKS-Cluster ein

Verwenden Sie diesen Ansatz, wenn Sie GuardDuty die Updates für den Security Agent nur für ausgewählte EKS-Cluster in Ihrem Konto bereitstellen und verwalten möchten. Bei dieser Methode

wird ein Tag-basierter [1]-Ansatz verwendet, bei dem Sie die EKS-Cluster markieren können, für die Sie Laufzeit-Ereignisse erhalten möchten.

Auswirkungen der Verwendung dieses Ansatzes

- Durch die Verwendung von Inklusion-Tags GuardDuty wird der Security Agent automatisch nur für die ausgewählten EKS-Cluster bereitgestellt und verwaltet, die mit`GuardDutyManaged`: `true` als Schlüssel-Wert-Paar gekennzeichnet sind.
- Dieser Ansatz hat auch die gleichen Auswirkungen, wie für Überwachen Sie alle EKS-Cluster angegeben.

Überlegungen

- Wenn der Wert des `GuardDutyManaged`-Tags nicht auf `true` festgelegt ist, funktioniert das Einschließen-Tag nicht wie erwartet, und dies kann sich auf die Überwachung Ihres EKS-Clusters auswirken.
- Um sicherzustellen, dass Ihre ausgewählten EKS-Cluster überwacht werden, müssen Sie verhindern, dass die Tags geändert werden, es sei denn, es handelt sich um vertrauenswürdige Identitäten.

  > **Important**
  >
  > Verwalten Sie die Berechtigungen zum Ändern des Werts des `GuardDutyManaged`-Tags für Ihren EKS-Cluster mithilfe von Service-Kontrollrichtlinie oder IAM-Richtlinien. Weitere Informationen finden Sie unter Service-Kontrollrichtlinien (SCPs) im Benutzerhandbuch für AWS Organizations oder Zugriff auf AWS -Ressourcen steuern im IAM-Benutzerhandbuch.

- Bei einem potenziell neuen EKS-Cluster, den Sie nicht überwachen möchten, stellen Sie sicher, dass Sie bei der Erstellung dieses EKS-Clusters das `false` Schlüssel-Wert-Paar`GuardDutyManaged`: hinzufügen.
- Bei diesem Ansatz werden auch dieselben Überlegungen berücksichtigt, wie für Überwachen Sie alle EKS-Cluster angegeben.

[1]Weitere Informationen zum Markieren von ausgewählten EKS-Clustern finden Sie unter Markieren Ihrer Amazon-EKS-Ressourcen im Amazon-EKS-Benutzerhandbuch.

Den GuardDuty Security Agent manuell verwalten

Verwenden Sie diesen Ansatz, wenn Sie den GuardDuty Security Agent manuell auf allen Ihren EKS-Clustern bereitstellen und verwalten möchten. Stellen Sie sicher, dass EKS-Laufzeit-Überwachung für Ihre Konten aktiviert ist. Der GuardDuty Security Agent funktioniert möglicherweise nicht wie erwartet, wenn Sie EKS Runtime Monitoring nicht aktivieren.

Auswirkungen der Verwendung dieses Ansatzes

Sie müssen die Bereitstellung des GuardDuty Security Agents in Ihren EKS-Clustern für alle Konten koordinieren und festlegen AWS-Regionen , wo diese Funktion verfügbar ist. Sie müssen auch die Agentenversion aktualisieren, wenn sie GuardDuty veröffentlicht wird. Weitere Informationen zu Agentenversionen für EKS finden Sie unterGuardDuty Security Agent-Versionen für Amazon EKS-Ressourcen.

Überlegungen

Sie müssen einen sicheren Datenfluss unterstützen und gleichzeitig Versorgungslücken überwachen und beheben, da kontinuierlich neue Cluster und Workloads bereitgestellt werden.

So funktioniert Runtime Monitoring mit Amazon EC2-Instances

Ihre Amazon EC2-Instances können mehrere Arten von Anwendungen und Workloads in Ihrer Umgebung ausführen. AWS Wenn Sie Runtime Monitoring aktivieren und den GuardDuty Security Agent verwalten, GuardDuty hilft er Ihnen dabei, Bedrohungen in Ihren vorhandenen und potenziell neuen Amazon EC2-Instances zu erkennen. Diese Funktion unterstützt auch Amazon ECS Managed EC2-Instances.

> **Note**
>
> Runtime Monitoring unterstützt keine Anwendungen, die auf Amazon ECS Managed Instances ausgeführt werden.

Wenn Sie Runtime Monitoring aktivieren, sind Sie GuardDuty bereit, Laufzeitereignisse aus aktuell laufenden und neuen Prozessen in Amazon EC2-Instances zu verarbeiten. GuardDuty erfordert einen Sicherheitsagenten, an den Laufzeitereignisse von Ihrer EC2-Instance gesendet werden. GuardDuty

Bei Amazon EC2-Instances arbeitet der GuardDuty Security Agent auf Instance-Ebene. Sie können entscheiden, ob Sie alle oder nur ausgewählte Amazon EC2-Instances in Ihrem Konto überwachen

möchten. Wenn Sie ausgewählte Instances verwalten möchten, ist der Security Agent nur für diese Instances erforderlich.

GuardDuty kann auch Laufzeitereignisse von neuen Aufgaben und bestehenden Aufgaben verarbeiten, die in Amazon EC2-Instances innerhalb von Amazon ECS-Clustern ausgeführt werden.

Um den GuardDuty Security Agent zu installieren, bietet Runtime Monitoring die folgenden zwei Optionen:

- Verwenden Sie die automatische Agentenkonfiguration (empfohlen), oder
- Den Security Agent manuell verwalten

Verwenden Sie die automatische Agentenkonfiguration über GuardDuty (empfohlen)

Verwenden Sie eine automatisierte Agentenkonfiguration, die es GuardDuty ermöglicht, den Security Agent in Ihrem Namen auf Ihren Amazon EC2-Instances zu installieren. GuardDuty verwaltet auch die Updates für den Security Agent.

GuardDuty Installiert den Security Agent standardmäßig auf allen Instances in Ihrem Konto. Wenn Sie den Security Agent nur für ausgewählte EC2-Instances installieren und verwalten möchten GuardDuty , fügen Sie Ihren EC2-Instances nach Bedarf Inklusions- oder Ausschluss-Tags hinzu.

Manchmal möchten Sie möglicherweise nicht die Laufzeitereignisse für alle Amazon EC2-Instances überwachen, die zu Ihrem Konto gehören. In Fällen, in denen Sie die Laufzeitereignisse für eine begrenzte Anzahl von Instances überwachen möchten, fügen Sie diesen ausgewählten Instances ein Inklusion-Tag als`GuardDutyManaged`: `true` hinzu. Beginnend mit der Verfügbarkeit der automatisierten Agentenkonfiguration für Amazon EC2 gilt: Wenn Ihre EC2-Instance über ein Inklusion-Tag (`GuardDutyManaged`:`true`) verfügt, GuardDuty das Tag und verwaltet den Security Agent für die ausgewählten Instances, auch wenn Sie die automatische Agentenkonfiguration nicht explizit aktivieren.

Wenn es andererseits eine begrenzte Anzahl von EC2-Instances gibt, für die Sie keine Laufzeitereignisse überwachen möchten, fügen Sie diesen ausgewählten Instances ein Ausschluss-Tag (`GuardDutyManaged`:`false`) hinzu. GuardDuty berücksichtigt das Ausschluss-Tag, indem es den Security Agent für diese EC2-Ressourcen weder installiert noch verwaltet.

Auswirkung

Wenn Sie die automatische Agentenkonfiguration in einer AWS-Konto oder einer Organisation verwenden, gestatten GuardDuty Sie, die folgenden Schritte in Ihrem Namen durchzuführen:

- GuardDuty erstellt eine SSM-Verknüpfung für alle Ihre Amazon EC2-Instances, die über SSM verwaltet werden und in der Konsole unter Fleet Manager angezeigt werden. https://console.aws.amazon.com/systems-manager/
- Verwendung von Inklusion-Tags bei deaktivierter automatisierter Agentenkonfiguration — Wenn Sie nach der Aktivierung von Runtime Monitoring die automatische Agentenkonfiguration nicht aktivieren, sondern Ihrer Amazon EC2-Instance das Inklusions-Tag hinzufügen, bedeutet dies, dass Sie die Erlaubnis haben, den Security Agent in Ihrem Namen GuardDuty zu verwalten. Die SSM-Zuordnung installiert dann den Security Agent in jeder Instance, die das Inklusions-Tag (:) `GuardDutyManaged` hat. `true`
- Wenn Sie die automatische Agentenkonfiguration aktivieren — Die SSM-Zuordnung installiert dann den Security Agent auf allen EC2-Instances, die zu Ihrem Konto gehören.
- Verwendung von Ausschlusstags bei automatisierter Agentenkonfiguration — Bevor Sie die automatische Agentenkonfiguration aktivieren, bedeutet das Hinzufügen eines Ausschluss-Tags zu Ihrer Amazon EC2-Instance, dass Sie die Installation und Verwaltung des Security Agents für diese ausgewählte Instance verhindern. GuardDuty

  Wenn Sie nun die automatische Agentenkonfiguration aktivieren, installiert und verwaltet die SSM-Zuordnung den Security Agent in allen EC2-Instances mit Ausnahme derjenigen, die mit dem Ausschluss-Tag gekennzeichnet sind.
- GuardDuty erstellt VPC-Endpunkte in allen VPCs, einschließlich gemeinsam genutzter VPCs, sofern sich in dieser VPC mindestens eine Linux EC2-Instance befindet, die sich nicht im Instance-Status „Beendet“ oder „Herunterfahren“ befindet. Dazu gehören die zentralisierte VPC und die Spoke-VPCs. GuardDuty unterstützt nicht die Erstellung eines VPC-Endpunkts nur für die zentralisierte VPC. Weitere Informationen zur Funktionsweise der zentralisierten VPC finden Sie unter Interface VPC Endpoints im AWS Whitepaper — Aufbau einer skalierbaren und sicheren Netzwerkinfrastruktur. Multi-VPC AWS

  Informationen zu den verschiedenen Instance-Status finden Sie unter Instance-Lebenszyklus im Amazon EC2-Benutzerhandbuch.

  GuardDuty unterstützt Verwenden von gemeinsam genutzter VPC mit Runtime Monitoring auch. Wenn alle Voraussetzungen für Ihr Unternehmen erfüllt sind AWS-Konto, GuardDuty wird die gemeinsam genutzte VPC zum Empfangen von Laufzeitereignissen verwendet.

> **Note**
>
> Für die Nutzung des VPC-Endpunkts fallen keine zusätzlichen Kosten an.

- Erstellt zusammen mit dem VPC-Endpunkt GuardDuty auch eine neue Sicherheitsgruppe. Die Regeln für eingehenden Verkehr (Eingangsregeln) steuern den Datenverkehr, der die Ressourcen erreichen darf, die der Sicherheitsgruppe zugeordnet sind. GuardDuty fügt Regeln für eingehenden Verkehr hinzu, die dem VPC-CIDR-Bereich für Ihre Ressource entsprechen, und passt sich diesen an, wenn sich der CIDR-Bereich ändert. Weitere Informationen finden Sie unter VPC-CIDR-Bereich im Amazon VPC-Benutzerhandbuch.

Den Security Agent manuell verwalten

Es gibt zwei Möglichkeiten, den Security Agent für Amazon EC2 manuell zu verwalten:

- Verwenden Sie GuardDuty verwaltete Dokumente in AWS Systems Manager , um den Security Agent auf Ihren Amazon EC2-Instances zu installieren, die bereits SSM-verwaltet werden.

  Wenn Sie eine neue Amazon EC2-Instance starten, stellen Sie sicher, dass SSM aktiviert ist.
- Verwenden Sie RPM Package Manager (RPM) -Skripts, um den Security Agent auf Ihren Amazon EC2-Instances zu installieren, unabhängig davon, ob diese SSM-verwaltet werden oder nicht.

Nächster Schritt

Informationen zu den ersten Schritten mit der Runtime Monitoring-Konfiguration zur Überwachung Ihrer Amazon EC2-Instances finden Sie unter. Voraussetzungen für die Unterstützung von Amazon EC2-Instances

So funktioniert Runtime Monitoring mit Fargate (nur Amazon ECS)

Wenn Sie Runtime Monitoring aktivieren, ist GuardDuty es bereit, die Laufzeitereignisse einer Aufgabe zu verarbeiten. Diese Aufgaben werden innerhalb der Amazon ECS-Cluster ausgeführt, die wiederum auf den AWS Fargate Instances ausgeführt werden. GuardDuty Um diese Laufzeitereignisse zu empfangen, müssen Sie den vollständig verwalteten, dedizierten Sicherheitsagenten verwenden.

> **Note**
>
> Runtime Monitoring unterstützt keine Anwendungen, die auf Amazon ECS Managed Instances ausgeführt werden.

Sie können zulassen GuardDuty , dass der GuardDuty Security Agent in Ihrem Namen verwaltet wird, indem Sie die automatisierte Agentenkonfiguration für ein AWS Konto oder eine Organisation verwenden. GuardDuty beginnt mit der Bereitstellung des Security Agents für die neuen Fargate-Aufgaben, die in Ihren Amazon ECS-Clustern gestartet werden. Die folgende Liste gibt an, was Sie erwartet, wenn Sie den GuardDuty Security Agent aktivieren.

Auswirkungen der Aktivierung des GuardDuty Security Agents

GuardDuty erstellt einen Virtual Private Cloud (VPC) -Endpunkt und eine Sicherheitsgruppe

- Wenn Sie den GuardDuty Security Agent bereitstellen, GuardDuty wird ein VPC-Endpunkt erstellt, über den der Security Agent die Laufzeitereignisse übermittelt. GuardDuty

  Erstellt zusammen mit dem VPC-Endpunkt GuardDuty auch eine neue Sicherheitsgruppe. Die Regeln für eingehenden Verkehr (Eingangsregeln) steuern den Datenverkehr, der die Ressourcen erreichen darf, die der Sicherheitsgruppe zugeordnet sind. GuardDuty fügt Regeln für eingehenden Verkehr hinzu, die dem VPC-CIDR-Bereich für Ihre Ressource entsprechen, und passt sich diesen an, wenn sich der CIDR-Bereich ändert. Weitere Informationen finden Sie unter VPC-CIDR-Bereich im Amazon VPC-Benutzerhandbuch.
- Arbeiten mit zentralisierter VPC mit automatisiertem Agenten — Wenn Sie die GuardDuty automatische Agentenkonfiguration für einen Ressourcentyp verwenden, GuardDuty wird in Ihrem Namen ein VPC-Endpunkt für alle VPCs erstellt. Dazu gehören die zentralisierte VPC und die Spoke-VPCs. GuardDutyunterstützt nicht die Erstellung eines VPC-Endpunkts nur für die zentralisierte VPC. Weitere Informationen zur Funktionsweise der zentralisierten VPC finden Sie unter Interface VPC Endpoints im AWS Whitepaper — Aufbau einer skalierbaren und sicheren Netzwerkinfrastruktur. Multi-VPC AWS
- Für die Nutzung des VPC-Endpunkts fallen keine zusätzlichen Kosten an.

GuardDuty fügt einen Beiwagen-Container hinzu

Für eine neue Fargate-Aufgabe oder einen neuen Fargate-Dienst, der gestartet wird, fügt sich ein GuardDuty Container (Sidecar) an jeden Container innerhalb der Amazon ECS Fargate-Aufgabe an. Der GuardDuty Security Agent wird innerhalb des angehängten Containers ausgeführt.

GuardDuty Dies hilft dabei GuardDuty , die Laufzeitereignisse jedes Containers zu erfassen, der im Rahmen dieser Aufgaben ausgeführt wird.

Das GuardDuty Sidecar-Container-Image wird in Amazon Elastic Container Registry (Amazon ECR) gespeichert, und die Bildebenen werden in Amazon S3 gespeichert. Wenn Ihre Aufgabe beginnt, muss sie dieses Bild aus ECR abrufen. Abhängig von Ihrer Netzwerkkonfiguration sind hierfür möglicherweise spezielle Einstellungen erforderlich, um den Zugriff auf ECR und S3 sicherzustellen. Wenn Sie beispielsweise Sicherheitsgruppen mit eingeschränktem Zugriff verwenden, müssen Sie den Zugriff auf die verwaltete S3-Präfixliste zulassen. Weitere Information dazu finden Sie unter Voraussetzungen für den Zugriff auf Container-Images.

Wenn Sie eine Fargate-Aufgabe starten und der GuardDuty Container (Sidecar) nicht in einem fehlerfreien Zustand gestartet werden kann, ist Runtime Monitoring so konzipiert, dass die Ausführung der Aufgaben nicht verhindert wird.

Standardmäßig ist eine Fargate-Aufgabe unveränderlich. GuardDuty stellt den Sidecar nicht bereit, wenn sich eine Aufgabe bereits in einem laufenden Zustand befindet. Wenn Sie einen Container in einer bereits laufenden Aufgabe überwachen möchten, können Sie die Aufgabe beenden und erneut starten.

Ansätze zur Verwaltung von GuardDuty Sicherheitsagenten in ECS-Fargate Amazon-Ressourcen

Runtime Monitoring bietet Ihnen die Möglichkeit, potenzielle Sicherheitsbedrohungen entweder auf allen Amazon ECS-Clustern (Kontoebene) oder auf ausgewählten Clustern (Cluster-Ebene) in Ihrem Konto zu erkennen. Wenn Sie die automatische Agentenkonfiguration für jede Amazon ECS Fargate-Aufgabe aktivieren, die ausgeführt wird, GuardDuty wird für jeden Container-Workload innerhalb dieser Aufgabe ein Sidecar-Container hinzugefügt. Der GuardDuty Security Agent wird in diesen Sidecar-Container eingesetzt. Auf diese Weise GuardDuty erhält er Einblick in das Laufzeitverhalten der Container in den Amazon ECS-Aufgaben.

Runtime Monitoring unterstützt die Verwaltung des Security Agents für Ihre Amazon ECS-Cluster (AWS Fargate) nur über GuardDuty. Die manuelle Verwaltung des Security Agents auf Amazon ECS-Clustern wird nicht unterstützt.

Bevor Sie Ihre Konten konfigurieren, sollten Sie prüfen, ob Sie das Laufzeitverhalten aller Container überwachen möchten, die zu den Amazon ECS-Aufgaben gehören, oder ob Sie bestimmte Ressourcen ein- oder ausschließen möchten. Ziehen Sie die folgenden Ansätze in Betracht.

Überwachen Sie alle Amazon ECS-Cluster

Dieser Ansatz hilft Ihnen dabei, potenzielle Sicherheitsbedrohungen auf Kontoebene zu erkennen. Verwenden Sie diesen Ansatz, wenn Sie potenzielle Sicherheitsbedrohungen für alle Amazon ECS-Cluster erkennen möchten GuardDuty , die zu Ihrem Konto gehören.

Schließen Sie bestimmte Amazon ECS-Cluster aus

Verwenden Sie diesen Ansatz, wenn GuardDuty Sie potenzielle Sicherheitsbedrohungen für die meisten Amazon ECS-Cluster in Ihrer AWS Umgebung erkennen, aber einige der Cluster ausschließen möchten. Dieser Ansatz hilft Ihnen, das Laufzeitverhalten der Container in Ihren Amazon ECS-Aufgaben auf Cluster-Ebene zu überwachen. Die Anzahl der Amazon ECS-Cluster, die zu Ihrem Konto gehören, beträgt beispielsweise 1000. Sie möchten jedoch nur 930 Amazon ECS-Cluster überwachen.

Bei diesem Ansatz müssen Sie den Amazon ECS-Clustern, die Sie nicht überwachen möchten, ein vordefiniertes GuardDuty Tag hinzufügen. Weitere Informationen finden Sie unter Verwaltung des automatisierten Sicherheitsagenten für Fargate (nur Amazon ECS).

Schließen Sie bestimmte Amazon ECS-Cluster ein

Verwenden Sie diesen Ansatz, wenn GuardDuty Sie potenzielle Sicherheitsbedrohungen für einige der Amazon ECS-Cluster erkennen möchten. Dieser Ansatz hilft Ihnen, das Laufzeitverhalten der Container innerhalb Ihrer Amazon ECS-Aufgaben auf Cluster-Ebene zu überwachen. Die Anzahl der Amazon ECS-Cluster, die zu Ihrem Konto gehören, beträgt beispielsweise 1000. Sie möchten jedoch nur 230 Cluster überwachen.

Bei diesem Ansatz müssen Sie den Amazon ECS-Clustern, die Sie überwachen möchten, ein vordefiniertes GuardDuty Tag hinzufügen. Weitere Informationen finden Sie unter Verwaltung des automatisierten Sicherheitsagenten für Fargate (nur Amazon ECS).

Nachdem Sie Runtime Monitoring aktiviert haben

Nachdem Sie Runtime Monitoring aktiviert und den GuardDuty Security Agent in Ihrem eigenständigen Konto oder mehreren Mitgliedskonten installiert haben, können Sie mit den folgenden Schritten sicherstellen, dass die Schutzplan-Einstellung wie erwartet funktioniert, und überwachen, wie viel Speicher und CPU der GuardDuty Security Agent verwendet.

Beurteilen Sie die Laufzeitabdeckung

GuardDuty empfiehlt Ihnen, den Abdeckungsstatus der Ressource, für die Sie den Security Agent eingesetzt haben, kontinuierlich zu überprüfen. Der Abdeckungsstatus kann entweder „Gesund“ oder „Ungesund“ lauten. Der Deckungsstatus Fehlerhaft gibt an, dass GuardDuty bei einer Aktivität auf Betriebssystemebene die Laufzeitereignisse von der entsprechenden Ressource empfangen werden.

Wenn der Abdeckungsstatus für die Ressource auf Fehlerfrei gesetzt GuardDuty wird, kann sie die Laufzeitereignisse empfangen und analysieren, um eine Bedrohung zu erkennen. Wenn in den Aufgaben oder Anwendungen, die in Ihren Containern ausgeführt werden, eine potenzielle Sicherheitsbedrohung GuardDuty erkannt wird, werden Workloads und Instances GuardDuty generiertGuardDuty Findetypen für die Laufzeitüberwachung.

Sie können Amazon EventBridge (EventBridge) auch so konfigurieren, dass es eine Benachrichtigung erhält, wenn sich der Deckungsstatus von Ungesund zu Gesund und auf andere Weise ändert. Weitere Informationen finden Sie unter Überprüfung der Statistiken zur Laufzeitabdeckung und Behebung von Problemen.

Richten Sie die CPU- und Speicherüberwachung für den GuardDuty Security Agent ein

Nachdem Sie festgestellt haben, dass der Abdeckungsstatus als Fehlerfrei angezeigt wird, können Sie die Leistung des Security Agents für Ihren Ressourcentyp bewerten. GuardDuty Unterstützt für Amazon EKS-Cluster mit der Security Agent-Version v1.5 oder höher die Konfiguration der Parameter des (zusätzlichen) Security Agents. Weitere Informationen finden Sie unter Einrichten der CPU- und Arbeitsspeicherüberwachung.

GuardDuty erkennt potenzielle Bedrohungen

Sobald der Empfang der Laufzeitereignisse für Ihre Ressource GuardDuty beginnt, beginnt es mit der Analyse dieser Ereignisse. Wenn in einer Ihrer Amazon EC2-Instances, Amazon ECS-Cluster oder Amazon EKS-Cluster eine potenzielle Sicherheitsbedrohung GuardDuty erkannt wird, generiert es eine oder mehrereGuardDuty Findetypen für die Laufzeitüberwachung. Sie können auf die Ergebnisdetails zugreifen, um die betroffenen Ressourcendetails einzusehen.

Wie funktioniert die kostenlose 30-Tage-Testversion in Runtime Monitoring

Die 30-tägige kostenlose Testphase funktioniert unterschiedlich für die neuen GuardDuty Konten und die vorhandenen Konten, für die EKS Runtime Monitoring bereits aktiviert war, bevor die Runtime

Monitoring-Funktion auf Amazon EC2-Instances erweitert wurde, und AWS Fargate (nur Amazon ECS).

Ich verwende den GuardDuty Testzeitraum oder habe EKS Runtime Monitoring noch nie aktiviert

Die folgende Liste erklärt, wie die kostenlose 30-Tage-Testphase funktioniert, wenn Sie entweder die GuardDuty 30-tägige Testphase verwenden oder EKS Runtime Monitoring noch nie aktiviert haben:

- Wenn Sie Runtime Monitoring und EKS Runtime Monitoring GuardDuty zum ersten Mal aktivieren, werden sie standardmäßig nicht aktiviert.

  Wenn Sie Runtime Monitoring für Ihr Konto oder Ihre Organisation aktivieren, stellen Sie sicher, dass Sie auch den GuardDuty Security Agent für die Ressource konfigurieren, die Sie im Hinblick auf die Erkennung von Bedrohungen überwachen möchten. Wenn Sie beispielsweise Runtime Monitoring für Ihre Amazon EC2-Instances verwenden möchten, müssen Sie nach der Aktivierung von Runtime Monitoring auch den Security Agent für Amazon EC2 konfigurieren. Sie können wählen, ob Sie dies entweder manuell oder automatisch über tun möchten. GuardDuty
- Der Runtime Monitoring-Schutzplan ist auf Kontoebene aktiviert. Die 30-tägige kostenlose Testphase funktioniert auf Ressourcenebene. Nachdem der GuardDuty Security Agent auf einen bestimmten Ressourcentyp installiert wurde, beginnt die kostenlose 30-Tage-Testversion, sobald GuardDuty das erste Runtime-Ereignis für diesen Ressourcentyp eingeht. Sie haben den GuardDuty Agenten beispielsweise auf Ressourcenebene bereitgestellt (für Amazon EC2-Instance, Amazon ECS-Cluster und Amazon EKS-Cluster). Wenn das GuardDuty erste Laufzeitereignis für eine Amazon EC2-Instance eingeht, beginnt die kostenlose 30-Tage-Testversion nur für Amazon EC2.
- Wenn Sie nur EKS Runtime Monitoring aktivieren möchten — Wenn Sie EKS Runtime Monitoring GuardDuty zum ersten Mal aktivieren, ist EKS Runtime Monitoring standardmäßig nicht aktiviert (nach der Veröffentlichung von Runtime Monitoring). Sie müssen EKS Runtime Monitoring aktivieren. Um es optimal zu nutzen, stellen Sie sicher, dass Sie den GuardDuty Security Agent entweder manuell verwalten oder die automatische Agentenkonfiguration aktivieren, sodass der Agent in Ihrem Namen GuardDuty verwaltet wird. Ihre kostenlose 30-tägige Testphase für EKS Runtime Monitoring beginnt, wenn GuardDuty das erste Laufzeitereignis für die Amazon EKS-Ressource eingeht.

Ich habe EKS Runtime Monitoring vor dem Start von Runtime Monitoring aktiviert

Verwenden Sie diesen Abschnitt nur, wenn EKS Runtime Monitoring für Sie AWS-Konto aktiviert war und Sie jetzt zu Runtime Monitoring migrieren möchten.

Die folgende Liste enthält Szenarien, die auf Ihren Anwendungsfall der Aktivierung von Runtime Monitoring zutreffen könnten:

- Für ein vorhandenes GuardDuty Konto, für das der EKS Runtime Monitoring-Schutzplan aktiviert ist und das die GuardDuty Konsolenerfahrung verwendet, um diesen Schutzplan zu verwenden — Mit der Ankündigung von Runtime Monitoring wurde die Erfahrung mit der EKS Runtime Monitoring-Konsole nun in Runtime Monitoring konsolidiert. Ihre bestehende Konfiguration für EKS Runtime Monitoring bleibt unverändert. Sie können den API/CLI Support weiterhin verwenden, um Vorgänge im Zusammenhang mit EKS Runtime Monitoring auszuführen.
- Um EKS Runtime Monitoring als Teil von Runtime Monitoring zu verwenden, müssen Sie Runtime Monitoring für Ihr Konto oder Ihre Organisation konfigurieren. Informationen zur Beibehaltung derselben Konfiguration für Runtime Monitoring finden Sie unterMigrieren von EKS Runtime Monitoring zu Runtime Monitoring. Dies hat jedoch keine Auswirkungen auf Ihre kostenlose 30-Tage-Testversion für die Amazon EKS-Ressource.
- Der Runtime Monitoring-Schutzplan ist auf Kontoebene pro Region aktiviert. Nachdem der GuardDuty Security Agent für einen der angegebenen Ressourcentypen (Amazon EC2-Instance und Amazon ECS-Cluster) bereitgestellt wurde, beginnt die kostenlose 30-Tage-Testversion, sobald das erste mit GuardDuty der Ressource verknüpfte Laufzeitereignis eingeht. Jedem Ressourcentyp ist eine kostenlose 30-Tage-Testversion zugeordnet.

  Beispiel: Nachdem Sie Runtime Monitoring aktiviert haben, entscheiden Sie sich dafür, den GuardDuty Agenten nur auf der Amazon EC2-Instance bereitzustellen. Die kostenlose 30-Tage-Testversion für diese Ressource beginnt erst, wenn GuardDuty das erste Laufzeitereignis für eine Amazon EC2-Instance eingeht. Später, wenn Sie den GuardDuty Agenten für Fargate (nur Amazon ECS) bereitstellen, beginnt die kostenlose 30-Tage-Testversion für diese Ressource erst, wenn das erste Laufzeitereignis für den Amazon ECS-Cluster GuardDuty empfangen wird. Da Sie EKS Runtime Monitoring bereits für Ihr Konto aktiviert haben, wird die kostenlose 30-Tage-Testversion für eine Amazon EKS-Ressource GuardDuty nicht zurückgesetzt.

Voraussetzungen für die Aktivierung von Runtime Monitoring

Um Runtime Monitoring zu aktivieren und den GuardDuty Security Agent zu verwalten, müssen Sie die Voraussetzungen für jeden Ressourcentyp erfüllen, den Sie im Hinblick auf die Erkennung einer Bedrohung überwachen möchten. Für jeden Ressourcentyp gelten unterschiedliche Voraussetzungen. GuardDuty Unterstützt beispielsweise verschiedene Betriebssystemverteilungen, die auf dem Ressourcentyp basieren.

Wenn Sie nur Amazon EC2-Ressourcen überwachen möchten, beachten Sie die Voraussetzungen für Amazon EC2-Instances. Wenn Sie sich zu einem späteren Zeitpunkt dafür entscheiden, Amazon EKS-Ressourcen zu überwachen, müssen Sie die für Amazon EKS-Cluster spezifischen Voraussetzungen erfüllen.

Die folgenden Abschnitte enthalten Voraussetzungen, die auf dem Ressourcentyp basieren.

Inhalt

- Voraussetzungen für die Unterstützung von Amazon EC2-Instances
- Voraussetzungen für die ECS-EC2 Bottlerocket-Unterstützung
- Voraussetzungen für AWS Fargate Unterstützung (nur Amazon ECS)
- Voraussetzungen für die Unterstützung von Amazon EKS-Clustern

Voraussetzungen für die Unterstützung von Amazon EC2-Instances

Dieser Abschnitt enthält die Voraussetzungen für die Überwachung des Laufzeitverhaltens Ihrer Amazon EC2-Instances. Nachdem diese Voraussetzungen erfüllt sind, finden Sie weitere Informationen unterLaufzeitüberwachung aktivieren GuardDuty.

Themen

- Stellen Sie sicher, dass EC2-Instances SSM-verwaltet werden (nur für die automatische Agentenkonfiguration)
- Überprüfen Sie die architektonischen Anforderungen
- Validierung der Service Control-Richtlinie Ihres Unternehmens in einer Umgebung mit mehreren Konten
- Bei Verwendung der automatisierten Agentenkonfiguration
- CPU- und Speicherlimit für Agenten GuardDuty

- Nächster Schritt

Stellen Sie sicher, dass EC2-Instances SSM-verwaltet werden (nur für die automatische Agentenkonfiguration)

GuardDuty verwendet AWS Systems Manager (SSM), um den Security Agent automatisch auf Ihren Instances bereitzustellen, zu installieren und zu verwalten. Wenn Sie vorhaben, den GuardDuty Agenten manuell zu installieren und zu verwalten, ist SSM nicht erforderlich.

Informationen zur Verwaltung Ihrer Amazon EC2-Instances mit Systems Manager mit Systems Manager für Amazon EC2-Instances finden Sie https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-setting-up-ec2.html im AWS Systems Manager Benutzerhandbuch.

Überprüfen Sie die architektonischen Anforderungen

Die Architektur Ihrer Betriebssystemverteilung kann sich auf das Verhalten des GuardDuty Security Agents auswirken. Sie müssen die folgenden Anforderungen erfüllen, bevor Sie Runtime Monitoring für Amazon EC2-Instances verwenden können:

- Die Kernel-Unterstützung umfasste`BPF`, `Tracepoints` und`Kprobe`. Für CPU-Architekturen unterstützt Runtime Monitoring AMD64 (`x64`) und ARM64 (Graviton2 und höher). [1]

  Die folgende Tabelle zeigt die Betriebssystemverteilung, die verifiziert wurde, um den GuardDuty Security Agent für Amazon EC2-Instances zu unterstützen.

Verteilung des Betriebssystems [2]	Kernel-Version [3]
Amazon Linux 2	5.4 [4], 5.10 [4], 5.15
Amazon Linux 2023	5,4 [4], 5,10, 5,15 [4], 6,1, 6,5, 6,8, 6,12
Ubuntu 20.04, 22.04, 24.04, 26.04	5.4 [4], 5.10, 5.15, 6.1 [4], 6.5, 6.8, 6.13, 6.14, 7.0
Debian 11, 12, 13	5.4 [4], 5.10 [4], 5.15, 6.1, 6.5, 6.8, 6.12

Verteilung des Betriebssystems [2]	Kernel-Version [3]
RedHat 9,4, 10,2	5,14, 6,12
Fedora 34, 40, 41, 43, 44	5,11, 5,17, 6,8, 6,12, 7,1
CentOS Stream 9, 10	5,14, 6,12
Oracle Linux 8.9, 9.3	5,15
Rocky Linux 9.5, 10.1	5,14, 6,12
Alma Linux 9, 10	5,14, 6,12
SUSE Linux Enterprise Server 16	6.12

1. Die Laufzeitüberwachung für Amazon EC2-Ressourcen unterstützt Graviton-Instances der ersten Generation wie A1-Instance-Typen nicht.
2. Unterstützung für verschiedene Betriebssysteme — GuardDuty hat die Runtime Monitoring-Unterstützung für die in der vorherigen Tabelle aufgeführte Betriebsdistribution verifiziert. Obwohl der GuardDuty Security Agent möglicherweise auf Betriebssystemen läuft, die in der vorherigen Tabelle nicht aufgeführt sind, kann das GuardDuty Team den erwarteten Sicherheitswert nicht garantieren.
3. Für jede Kernelversion müssen Sie das `CONFIG_DEBUG_INFO_BTF` Flag auf y (was wahr bedeutet) setzen. Dies ist erforderlich, damit der GuardDuty Security Agent wie erwartet ausgeführt werden kann.
4. Für Kernel-Versionen 5.10 und früher verwendet der GuardDuty Security Agent den gesperrten Speicher im RAM (`RLIMIT_MEMLOCK`), um wie erwartet zu funktionieren. Wenn der `RLIMIT_MEMLOCK` Wert Ihres Systems zu niedrig eingestellt ist, GuardDuty empfiehlt, sowohl harte als auch weiche Grenzwerte auf mindestens 32 MB festzulegen. Informationen zum Überprüfen und Ändern des `RLIMIT_MEMLOCK` Standardwerts finden Sie unter RLIMIT_MEMLOCK-Werte anzeigen und aktualisieren .

- Zusätzliche Anforderungen — Nur wenn Sie Amazon ECS/Amazon EC2 haben

  Für Amazon ECS/Amazon EC2 empfehlen wir, die neuesten ECS-optimized Amazon-AMIs (vom 29. September 2023 oder später) oder die Amazon ECS-Agent-Version v1.77.0 zu verwenden.

RLIMIT_MEMLOCK-Werte anzeigen und aktualisieren

Wenn das `RLIMIT_MEMLOCK` Limit Ihres Systems zu niedrig eingestellt ist, funktioniert der GuardDuty Security Agent möglicherweise nicht wie vorgesehen. GuardDuty empfiehlt, dass sowohl die harten als auch die weichen Grenzwerte mindestens 32 MB betragen müssen. Wenn Sie die Grenzwerte nicht aktualisieren, können GuardDuty Sie die Laufzeitereignisse für Ihre Ressource nicht überwachen. Wenn die angegebenen Mindestgrenzen überschritten werden, `RLIMIT_MEMLOCK` ist es für Sie optional, diese Grenzwerte zu aktualisieren.

Sie können den `RLIMIT_MEMLOCK` Standardwert entweder vor oder nach der Installation des GuardDuty Security Agents ändern.

Um RLIMIT_MEMLOCK-Werte anzuzeigen

1. Führen Sie `ps aux | grep guardduty`. Dadurch wird die Prozess-ID () ausgegeben. `pid`
2. Kopieren Sie die Prozess-ID (`pid`) aus der Ausgabe des vorherigen Befehls.
3. Führen Sie den Befehl aus, `grep "Max locked memory" /proc/pid/limits` nachdem Sie den `pid` durch die aus dem vorherigen Schritt kopierte Prozess-ID ersetzt haben.

   Dadurch wird die maximale Anzahl an gesperrtem Speicher für die Ausführung des GuardDuty Security Agents angezeigt.

Um RLIMIT_MEMLOCK-Werte zu aktualisieren

1. Falls die `/etc/systemd/system.conf.d/NUMBER-limits.conf` Datei existiert, kommentieren Sie die Zeile von `DefaultLimitMEMLOCK` aus dieser Datei aus. Diese Datei legt einen Standard `RLIMIT_MEMLOCK` mit hoher Priorität fest, der Ihre Einstellungen in der `/etc/systemd/system.conf` Datei überschreibt.
2. Öffnen Sie die `/etc/systemd/system.conf` Datei und entkommentieren Sie die Zeile, in der sie steht. `#DefaultLimitMEMLOCK=`

3. Aktualisieren Sie den Standardwert, indem Sie sowohl harte als auch weiche `RLIMIT_MEMLOCK` Grenzwerte auf mindestens 32 MB angeben. Das Update sollte so aussehen:`DefaultLimitMEMLOCK=32M:32M`. Das Format ist `soft-limit:hard-limit`.
4. Führen Sie `sudo reboot`.

Validierung der Service Control-Richtlinie Ihres Unternehmens in einer Umgebung mit mehreren Konten

Wenn Sie eine Service Control Policy (SCP) zur Verwaltung von Berechtigungen in Ihrer Organisation eingerichtet haben, überprüfen Sie, ob die Berechtigungsgrenze die Aktion zulässt. `guardduty:SendSecurityTelemetry` GuardDuty benötigt diese Berechtigung, um die Laufzeitüberwachung für verschiedene Ressourcentypen zu unterstützen.

Wenn es sich bei Ihrem Konto um ein Mitgliedskonto handelt, wenden Sie sich an den entsprechenden delegierten Administrator. Informationen zur Verwaltung von SCPs für Ihre Organisation finden Sie unter Service Control Policies (SCPs).

Bei Verwendung der automatisierten Agentenkonfiguration

Dazu Verwenden Sie die automatische Agentenkonfiguration (empfohlen) AWS-Konto müssen Sie die folgenden Voraussetzungen erfüllen:

- Wenn Sie Inklusion-Tags mit automatisierter Agentenkonfiguration verwenden, GuardDuty um eine SSM-Zuordnung für eine neue Instance zu erstellen, stellen Sie sicher, dass die neue Instance von SSM verwaltet wird und in der https://console.aws.amazon.com/systems-manager/ Konsole unter Fleet Manager angezeigt wird.
- Wenn Sie Ausschluss-Tags mit automatisierter Agentenkonfiguration verwenden:
  - Fügen Sie das `false` Tag`GuardDutyManaged`: hinzu, bevor Sie den GuardDuty automatisierten Agenten für Ihr Konto konfigurieren.

    Stellen Sie sicher, dass Sie Ihren Amazon EC2-Instances das Ausschluss-Tag hinzufügen, bevor Sie sie starten. Sobald Sie die automatische Agentenkonfiguration für Amazon EC2 aktiviert haben, fällt jede EC2-Instance, die ohne Ausschluss-Tag gestartet wird, unter die GuardDuty automatische Agentenkonfiguration.
  - Aktivieren Sie die Einstellung „Tags in Metadaten zulassen“ für Ihre Instances. Diese Einstellung ist erforderlich, da das Ausschluss-Tag aus dem Instanz-Metadatendienst (IMDS) gelesen werden GuardDuty muss, um zu bestimmen, ob die Instanz von der Agenteninstallation

ausgeschlossen werden soll. Weitere Informationen finden Sie unter Aktivieren des Zugriffs auf Tags in Instance-Metadaten im Amazon EC2-Benutzerhandbuch.

CPU- und Speicherlimit für Agenten GuardDuty

CPU-Limit

GuardDuty begrenzt den Security Agent auf 10 Prozent der gesamten vCPU-Kapazität auf der Instance. Auf einer Instance mit 4 vCPU-Kernen kann der Agent beispielsweise maximal 0,4 vCPU verwenden.

Speicherlimit

Aus dem Speicher, der Ihrer Amazon EC2-Instance zugeordnet ist, gibt es einen begrenzten Speicher, den der GuardDuty Security Agent verwenden kann.

Die folgende Tabelle zeigt das Speicherlimit.

Speicher der Amazon EC2-Instance	Maximaler Speicher für den Agenten GuardDuty
Weniger als 8 GB	128 MB
8 GB bis weniger als 32 GB	256 MB
Mehr als oder gleich 32 GB	1 GB

Nächster Schritt

Der nächste Schritt ist die Konfiguration von Runtime Monitoring und die Verwaltung des Security Agents (automatisch oder manuell).

Voraussetzungen für die ECS-EC2 Bottlerocket-Unterstützung

Important

Dieser Abschnitt gilt nur für ECS-optimized Bottlerocket-AMIs *v1.62.1* und höher, einschließlich der folgenden Varianten:

- `bottlerocket-aws-ecs-2-x86_64` / `bottlerocket-aws-ecs-2-aarch64`

- `bottlerocket-aws-ecs-3-x86_64` / `bottlerocket-aws-ecs-3-aarch64`
- `bottlerocket-aws-ecs-2-nvidia` / `bottlerocket-aws-ecs-2-nvidia-fips`
- `bottlerocket-aws-ecs-3-nvidia` / `bottlerocket-aws-ecs-3-nvidia-fips`

Runtime Monitoring erweitert GuardDuty die Bedrohungserkennung auf Ihre Bottlerocket Amazon EC2-Instances in Amazon ECS-Clustern. Dabei wird ein Sicherheitsagent verwendet, der als Host-Container ausgeführt wird, um dem containeroptimierten Design von Bottlerocket zu entsprechen. Um es zu aktivieren, müssen Sie die Voraussetzungen in diesem Abschnitt erfüllen. Wenn diese Voraussetzungen erfüllt sind, finden Sie weitere Informationen unterLaufzeitüberwachung aktivieren GuardDuty.

Weitere Informationen zu Anforderungen und Anweisungen finden Sie unterVerwaltung des GuardDuty Sicherheitsagenten auf Bottlerocket (Amazon ECS auf Amazon EC2).

Themen

- Sorgen Sie dafür, dass EC2-Instances von SSM verwaltet werden, und konfigurieren Sie Instance-Berechtigungen
- Validierung der architektonischen Anforderungen
- Anforderungen an die Netzwerkkonnektivität
- Validierung der Service Control-Richtlinie Ihres Unternehmens in einer Umgebung mit mehreren Konten
- Bei Verwendung der automatisierten Agentenkonfiguration
- CPU- und Speicherlimit für Agenten GuardDuty
- Nächster Schritt

Sorgen Sie dafür, dass EC2-Instances von SSM verwaltet werden, und konfigurieren Sie Instance-Berechtigungen

GuardDuty verwendet AWS Systems Manager (SSM), um den Security Agent auf Ihren Bottlerocket-Instances bereitzustellen, zu installieren und zu verwalten. Dabei wird der SSM-Agent im Bottlerocket-Control-Container ausgeführt.

In den meisten Fällen decken die Berechtigungen, die Ihre Instances bereits für Bottlerocket haben, auch ab. GuardDuty Es sind keine zusätzlichen Richtlinien erforderlich. Die

`AmazonEC2ContainerRegistryReadOnly` Richtlinie, die Bottlerocket verwendet, um seine Kontroll- und Admin-Container-Images abzurufen, erfüllt auch die Anforderung, das GuardDuty Agenten-Container-Image abzurufen. Weitere Informationen finden Sie in der Bottlerocket-README-Datei. https://github.com/bottlerocket-os/bottlerocket/blob/develop/README.md#exploration

Das Instanzprofil muss die folgenden verwalteten Richtlinien enthalten:

- `AmazonSSMManagedInstanceCore`— Erforderlich, damit der Bottlerocket Control-Container den SSM-Agenten ausführen kann. Informationen zur Verwaltung Ihrer Amazon EC2-Instances mit Systems Manager mit Systems Manager für Amazon EC2-Instances finden Sie im Benutzerhandbuch. AWS Systems Manager
- `AmazonEC2ContainerRegistryReadOnly`— Erforderlich, um das GuardDuty Agenten-Container-Image aus Amazon ECR abzurufen. Es sind mindestens die folgenden Berechtigungen erforderlich:

```
...
      "ecr:GetAuthorizationToken",
      "ecr:BatchCheckLayerAvailability",
      "ecr:GetDownloadUrlForLayer",
      "ecr:BatchGetImage",
...
```

Um die Amazon ECR-Berechtigungen weiter einzuschränken, können Sie die Amazon ECR-Repository-URI hinzufügen, die den GuardDuty Sicherheitsagenten für Amazon ECS-Amazon EC2 Bottlerocket hostet. Weitere Informationen finden Sie unter ECR-Repository für GuardDuty Agenten auf Bottlerocket ECS-EC2.

Validierung der architektonischen Anforderungen

Die Architektur Ihrer Instances bestimmt, wie sich der Security Agent verhält. GuardDuty Bottlerocket ECS-2 und seine ECS-3 Varianten erfüllen diese Anforderungen sofort. Bestätigen Sie Folgendes, bevor Sie Runtime Monitoring aktivieren:

- Die Kernel-Unterstützung umfasst `eBPFTracepoints`, und`Kprobe`. ECS-2 Bottlerocket-Varianten verwenden den Kernel `6.1` und ECS-3 Varianten verwenden den Kernel. `6.12` Beide Versionen erfüllen die Kernel-Anforderungen für Runtime Monitoring. Die `CONFIG_DEBUG_INFO_BTF=y` Kernel-Option ist in Bottlerocket ECS-2 und Kernels standardmäßig aktiviert. ECS-3
- Für CPU-Architekturen unterstützt Runtime Monitoring AMD64 () und ARM64 (). `x86_64` `aarch64`

Anforderungen an die Netzwerkkonnektivität

GuardDuty hostet seinen Security Agent als Container-Image in Amazon ECR, sodass Ihre Instances eine Netzwerkverbindung zu Amazon ECR benötigen, um es abzurufen. Wählen Sie je nach Ihrer Netzwerkkonfiguration eine der folgenden Optionen:

Option 1 — Nutzung des öffentlichen Netzwerkzugriffs (falls verfügbar)

Wenn Ihre Bottlerocket-Instances in Subnetzen mit ausgehendem Internetzugang ausgeführt werden, ist keine zusätzliche Netzwerkkonfiguration erforderlich.

Option 2 — Verwendung von Amazon VPC-Endpunkten (für private Subnetze)

Für Bottlerocket-Instances in privaten Subnetzen bieten VPC-Endpunkte die Konnektivität, die der Agent benötigt. Konfigurieren Sie Endpunkte für Amazon ECR, Amazon S3 und Systems Manager, damit Instances das Agenten-Image abrufen und zur Bereitstellung mit Systems Manager kommunizieren können.

Weitere Informationen zur Konfiguration von VPC-Endpunkten finden Sie unter Erstellen der VPC-Endpunkte für Amazon ECR im Amazon Elastic Container Registry User Guide und Create VPC Endpoints im Benutzerhandbuch. AWS Systems Manager

Validierung der Service Control-Richtlinie Ihres Unternehmens in einer Umgebung mit mehreren Konten

Wenn Sie eine Service Control Policy (SCP) zur Verwaltung von Berechtigungen in Ihrer Organisation eingerichtet haben, überprüfen Sie, ob die Berechtigungsgrenze die Aktion zulässt. `guardduty:SendSecurityTelemetry` GuardDuty benötigt diese Berechtigung, um die Laufzeitüberwachung für verschiedene Ressourcentypen zu unterstützen.

Wenn es sich bei Ihrem Konto um ein Mitgliedskonto handelt, wenden Sie sich an den entsprechenden delegierten Administrator. Informationen zur Verwaltung von SCPs für Ihre Organisation finden Sie unter Service Control Policies (SCPs).

Bei Verwendung der automatisierten Agentenkonfiguration

Um die automatische Agentenkonfiguration verwenden zu können, AWS-Konto müssen Sie die folgenden Voraussetzungen erfüllen:

- Wenn Sie Inklusion-Tags mit automatisierter Agentenkonfiguration verwenden, GuardDuty um eine SSM-Zuordnung für eine neue Instanz zu erstellen, stellen Sie sicher, dass die neue Instanz von

SSM verwaltet wird und in der https://console.aws.amazon.com/systems-manager/ Konsole unter Fleet Manager angezeigt wird.

- Wenn Sie Ausschluss-Tags mit automatisierter Agentenkonfiguration verwenden:
  - Fügen Sie einer Amazon EC2-Instance das `false` Tag`GuardDutyManaged`: hinzu, bevor Sie sie starten und bevor Sie den GuardDuty automatisierten Agenten für Ihr Konto konfigurieren. Nachdem die automatische Agentenkonfiguration aktiviert wurde, wird jede Instance, die ohne Ausnahmetag gestartet wird, automatisch abgedeckt.
  - Aktivieren Sie für Ihre Instanzen die Einstellung „Tags in Metadaten zulassen“. Diese Einstellung ist erforderlich, da das Ausschluss-Tag aus dem Instanz-Metadatendienst (IMDS) gelesen werden GuardDuty muss, um zu bestimmen, ob die Instanz von der Agenteninstallation ausgeschlossen werden soll. Weitere Informationen finden Sie unter Aktivieren des Zugriffs auf Tags in Instance-Metadaten im Amazon EC2-Benutzerhandbuch.

CPU- und Speicherlimit für Agenten GuardDuty

CPU-Limit

GuardDuty begrenzt den Security Agent auf 10 Prozent der gesamten vCPU-Kapazität auf der Instance. Auf einer Instance mit 4 vCPU-Kernen kann der Agent beispielsweise maximal 0,4 vCPU verwenden.

Speicherlimit

Bezüglich des Speichers, der Ihrer Amazon EC2-Instance zugeordnet ist, gibt es ein Limit für den Speicher, den der GuardDuty Security Agent verwenden kann.

Die folgende Tabelle zeigt das Speicherlimit.

Speicher der Amazon EC2-Instance	Maximaler Speicher für den Agenten GuardDuty
Weniger als 8 GB	128 MB
8 GB bis weniger als 32 GB	256 MB
Mehr als oder gleich 32 GB	1 GB

Nächster Schritt

Im nächsten Schritt konfigurieren Sie Runtime Monitoring und verwalten den Security Agent automatisch.

Voraussetzungen für AWS Fargate Unterstützung (nur Amazon ECS)

Dieser Abschnitt enthält die Voraussetzungen für die Überwachung des Laufzeitverhaltens Ihrer Fargate-Amazon ECS-Ressourcen. Wenn diese Voraussetzungen erfüllt sind, finden Sie weitere Informationen unterLaufzeitüberwachung aktivieren GuardDuty.

Themen

- Validierung der architektonischen Anforderungen
- Voraussetzungen für den Zugriff auf Container-Images
- Validierung der Service Control-Richtlinie Ihres Unternehmens in einer Umgebung mit mehreren Konten
- Validierung der Rollenberechtigungen und der Grenzen der Richtlinienberechtigungen
- CPU- und Arbeitsspeicherlimits

Validierung der architektonischen Anforderungen

Die von Ihnen verwendete Plattform kann sich darauf auswirken, wie der GuardDuty Security Agent GuardDuty den Empfang der Laufzeitereignisse von Ihren Amazon ECS-Clustern unterstützt. Sie müssen bestätigen, dass Sie eine der verifizierten Plattformen verwenden.

Erste Überlegungen:

Die AWS Fargate Plattform für Ihre Amazon ECS-Cluster muss Linux sein. Die entsprechende Plattformversion muss mindestens `1.4.0` oder sein`LATEST`. Weitere Informationen zu den Plattformversionen finden Sie unter Linux-Plattformversionen im Amazon Elastic Container Service Developer Guide.

Die Windows-Plattformversionen werden noch nicht unterstützt.

Verifizierte Plattformen

Die Betriebssystemverteilung und die CPU-Architektur wirken sich auf den Support aus, der vom GuardDuty Security Agent bereitgestellt wird. Die folgende Tabelle zeigt die verifizierte Konfiguration für die Bereitstellung des GuardDuty Security Agents und die Konfiguration von Runtime Monitoring.

Verteilung des Betriebssystems [1]	Kernel-Unterstützung	CPU-Architektur x64 (AMD64)	CPU-Architektur Graviton (ARM64)
Linux	eBPF, Tracepoints, Kprobe	Unterstützt	Unterstützt

[1] Unterstützung für verschiedene Betriebssysteme — GuardDuty hat die Runtime Monitoring-Unterstützung für die in der vorherigen Tabelle aufgeführte Betriebsdistribution verifiziert. Obwohl der GuardDuty Security Agent möglicherweise auf Betriebssystemen läuft, die in der vorherigen Tabelle nicht aufgeführt sind, kann das GuardDuty Team den erwarteten Sicherheitswert nicht garantieren.

Voraussetzungen für den Zugriff auf Container-Images

Die folgenden Voraussetzungen helfen Ihnen beim Zugriff auf das GuardDuty Sidecar-Container-Image aus dem Amazon ECR-Repository.

Berechtigungsanforderungen

Für die Rolle zur Aufgabenausführung sind bestimmte Amazon Elastic Container Registry (Amazon ECR) -Berechtigungen erforderlich, um das GuardDuty Security Agent-Container-Image herunterzuladen:

```
...
      "ecr:GetAuthorizationToken",
      "ecr:BatchCheckLayerAvailability",
      "ecr:GetDownloadUrlForLayer",
      "ecr:BatchGetImage",
...
```

Um die Amazon ECR-Berechtigungen weiter einzuschränken, können Sie die Amazon ECR-Repository-URI hinzufügen, für die der GuardDuty Security Agent gehostet wird AWS Fargate (nur Amazon ECS). Weitere Informationen finden Sie unter Amazon ECR-Repository-Hosting-Agent GuardDuty.

Sie können entweder die AmazonECSTaskExecutionRolePolicy verwaltete Richtlinie verwenden oder die oben genannten Berechtigungen zu Ihrer `TaskExecutionRole` Richtlinie hinzufügen.

Konfiguration der Aufgabendefinition

Wenn Sie Amazon ECS-Services erstellen oder aktualisieren, müssen Sie Subnetzinformationen in Ihrer Aufgabendefinition angeben:

Für die Ausführung der UpdateService APIs CreateService und in der Amazon Elastic Container Service API-Referenz müssen Sie die Subnetzinformationen übergeben. Weitere Informationen finden Sie unter Amazon ECS-Aufgabendefinitionen im Amazon Elastic Container Service Developer Guide.

Anforderungen an die Netzwerkkonnektivität

Sie müssen die Netzwerkkonnektivität sicherstellen, um das GuardDuty Container-Image von Amazon ECR herunterzuladen. Diese Anforderung ist spezifisch für, GuardDuty da Amazon ECR zum Hosten seines Sicherheitsagenten verwendet wird. Abhängig von Ihrer Netzwerkkonfiguration müssen Sie eine der folgenden Optionen implementieren:

Option 1 — Nutzung des öffentlichen Netzwerkzugriffs (falls verfügbar)

Wenn Ihre Fargate-Aufgaben in Subnetzen mit ausgehendem Internetzugang ausgeführt werden, ist keine zusätzliche Netzwerkkonfiguration erforderlich.

Option 2 — Verwendung von Amazon VPC-Endpunkten (für private Subnetze)

Wenn Ihre Fargate-Aufgaben in privaten Subnetzen ohne Internetzugang ausgeführt werden, müssen Sie VPC-Endpunkte für ECR konfigurieren, um sicherzustellen, dass die ECR-Repository-URI, die den Security Agent hostet, über das Netzwerk zugänglich ist. GuardDuty Ohne diese Endpunkte können Aufgaben in privaten Subnetzen das Container-Image nicht herunterladen. GuardDuty

Anweisungen zur Einrichtung von VPC-Endpunkten finden Sie unter Erstellen der VPC-Endpunkte für Amazon ECR im Amazon Elastic Container Registry User Guide.

Informationen dazu, wie Sie Fargate das Herunterladen des GuardDuty Containers ermöglichen, finden Sie unter Verwenden von Amazon ECR-Images mit Amazon ECS im Amazon Elastic Container Registry Benutzerhandbuch.

Sicherheitsgruppenkonfiguration

Die GuardDuty Container-Images befinden sich in Amazon ECR und erfordern Amazon S3-Zugriff. Diese Anforderung gilt speziell für das Herunterladen von Container-Images von Amazon ECR. Für Aufgaben mit eingeschränktem Netzwerkzugriff müssen Sie Ihre Sicherheitsgruppen so konfigurieren, dass sie den Zugriff auf S3 ermöglichen.

Fügen Sie Ihrer Sicherheitsgruppe eine Regel für ausgehenden Datenverkehr hinzu, die den Datenverkehr zur verwalteten S3-Präfixliste (`pl-xxxxxxxx`) auf Port 443 zulässt. Informationen zum Hinzufügen einer Regel für ausgehenden Datenverkehr finden Sie unter Sicherheitsgruppenregeln konfigurieren im Amazon VPC-Benutzerhandbuch.

Informationen zum Anzeigen Ihrer AWS verwalteten Präfixlisten in der Konsole oder zur Beschreibung mithilfe von AWS Command Line Interface (AWS CLI) finden Sie unter AWS-managed Prefixlisten im Amazon VPC-Benutzerhandbuch.

Validierung der Service Control-Richtlinie Ihres Unternehmens in einer Umgebung mit mehreren Konten

In diesem Abschnitt wird erklärt, wie Sie Ihre SCP-Einstellungen (Service Control Policy) überprüfen, um sicherzustellen, dass Runtime Monitoring in Ihrem gesamten Unternehmen erwartungsgemäß funktioniert.

Wenn Sie eine oder mehrere Service Control-Richtlinien zur Verwaltung von Berechtigungen in Ihrer Organisation eingerichtet haben, müssen Sie sicherstellen, dass die `guardduty:SendSecurityTelemetry` Aktion nicht verweigert wird. Informationen zur Funktionsweise von SCPs finden Sie unter SCP-Evaluierung im AWS Organizations Benutzerhandbuch.

Wenn es sich bei Ihrem Konto um ein Mitgliedskonto handelt, wenden Sie sich an den entsprechenden delegierten Administrator. Informationen zur Verwaltung von SCPs für Ihr Unternehmen finden Sie im Benutzerhandbuch unter Service Control Policies (SCPs). AWS Organizations

Führen Sie die folgenden Schritte für alle SCPs aus, die Sie in Ihrer Umgebung mit mehreren Konten eingerichtet haben:

Um **`Guardduty: SendSecurityTelemetry`** wird in SCP nicht verweigert

1. Melden Sie sich in der Organisationskonsole unter an. https://console.aws.amazon.com/organizations/ Sie müssen sich als IAM-Rolle oder als Root-Benutzer (nicht empfohlen) im Verwaltungskonto der Organisation anmelden.
2. Wählen Sie im linken Navigationsbereich Policies (Richtlinien). Wählen Sie dann unter Unterstützte Richtlinientypen die Option Dienststeuerungsrichtlinien aus.
3. Wählen Sie auf der Seite Dienststeuerungsrichtlinien den Namen der Richtlinie aus, die Sie überprüfen möchten.
4. Sehen Sie sich auf der Detailseite der Richtlinie den Inhalt dieser Richtlinie an. Stellen Sie sicher, dass die `guardduty:SendSecurityTelemetry` Aktion nicht abgelehnt wird.

   Die folgende SCP-Richtlinie ist ein Beispiel dafür, wie die Aktion nicht verweigert werden kann: `guardduty:SendSecurityTelemetry`

   JSON

   ```
   {
       "Version":"2012-10-17",
       "Statement": [
           {
       "Effect": "Allow",
               "Action": [
                   "guardduty:SendSecurityTelemetry"
               ],
               "Resource": "*"
           }
       ]
   }
   ```

   Wenn Ihre Richtlinie diese Aktion ablehnt, müssen Sie die Richtlinie aktualisieren. Weitere Informationen finden Sie unter Aktualisieren einer Service-Kontrollrichtlinie (SCP) im AWS Organizations -Benutzerhandbuch.

Validierung der Rollenberechtigungen und der Grenzen der Richtlinienberechtigungen

Gehen Sie wie folgt vor, um zu überprüfen, ob die mit der Rolle und ihrer Richtlinie verknüpften Berechtigungsgrenzen die `guardduty:SendSecurityTelemetry` Aktionen nicht einschränken.

So zeigen Sie die Berechtigungsgrenzen für Rollen und die zugehörige Richtlinie an

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im linken Navigationsbereich unter Zugriffsverwaltung die Option Rollen aus.
3. Wählen Sie auf der Seite Rollen die Rolle aus*`TaskExecutionRole`*, die Sie möglicherweise erstellt haben.
4. Erweitern Sie auf der Seite der ausgewählten Rolle auf der Registerkarte Berechtigungen den Richtliniennamen, der dieser Rolle zugeordnet ist. Stellen Sie dann sicher, dass diese Richtlinie nicht einschränkt`guardduty:SendSecurityTelemetry`.
5. Wenn die Grenze für Berechtigungen festgelegt ist, erweitern Sie diesen Abschnitt. Erweitern Sie dann jede Richtlinie, um sicherzustellen, dass sie die `guardduty:SendSecurityTelemetry` Aktion nicht einschränkt. Die Richtlinie sollte in etwa so aussehenExample SCP policy.

   Führen Sie bei Bedarf eine der folgenden Aktionen aus:

   - Um die Richtlinie zu ändern, wählen Sie Bearbeiten aus. Aktualisieren Sie auf der Seite „Berechtigungen ändern“ für diese Richtlinie die Richtlinie im Richtlinien-Editor. Stellen Sie sicher, dass das JSON-Schema gültig bleibt. Wählen Sie anschließend Weiter. Anschließend können Sie die Änderungen überprüfen und speichern.
   - Um diese Berechtigungsgrenze zu ändern und eine andere Grenze auszuwählen, wählen Sie Grenze ändern aus.
   - Um diese Berechtigungsgrenze zu entfernen, wählen Sie Grenze entfernen aus.

   Informationen zur Verwaltung von Richtlinien finden Sie AWS Identity and Access Management im IAM-Benutzerhandbuch unter Richtlinien und Berechtigungen.

CPU- und Arbeitsspeicherlimits

In der Fargate-Aufgabendefinition müssen Sie den CPU- und Speicherwert auf Aufgabenebene angeben. Die folgende Tabelle zeigt die gültigen Kombinationen von CPU- und Speicherwerten auf

Taskebene sowie das entsprechende maximale Speicherlimit für den GuardDuty Security Agent für den Container. GuardDuty

CPU-Wert	Speicherwert	GuardDuty Maximales Speicherlimit für Agenten
256 (0,25 vCPU)	512 MiB, 1 GB, 2 GB	128 MB
512 (0,5 vCPU)	1 GB, 2 GB, 3 GB, 4 GB	
1024 (1 vCPU)	2 GB, 3 GB, 4 GB	
	5 GB, 6 GB, 7 GB, 8 GB	
2048 (2 vCPU)	Zwischen 4 GB und 16 GB in 1-GB-Schritten	
4096 (4 vCPU)	Zwischen 8 GB und 20 GB in Schritten von 1 GB	
8 192 (8 vCPU)	Zwischen 16 GB und 28 GB in Schritten von 4 GB	256 MB
	Zwischen 32 GB und 60 GB in Schritten von 4 GB	512 MB
16384 (16 vCPU)	Zwischen 32 GB und 120 GB in 8-GB-Schritten	1 GB

Nachdem Sie Runtime Monitoring aktiviert und festgestellt haben, dass der Abdeckungsstatus Ihres Clusters fehlerfrei ist , können Sie die Container-Insight-Metriken einrichten und anzeigen. Weitere Informationen finden Sie unter Überwachung auf dem Amazon ECS-Cluster einrichten.

Der nächste Schritt besteht darin, Runtime Monitoring und auch den Security Agent zu konfigurieren.

Voraussetzungen für die Unterstützung von Amazon EKS-Clustern

Dieser Abschnitt enthält die Voraussetzungen für die Überwachung des Laufzeitverhaltens Ihrer Amazon EKS-Ressourcen. Diese Voraussetzungen sind entscheidend, damit der GuardDuty

Agent erwartungsgemäß funktioniert. Wenn diese Voraussetzungen erfüllt sind, finden Sie weitere Informationen unter Laufzeitüberwachung aktivieren GuardDuty So beginnen Sie mit der Überwachung Ihrer Ressourcen.

Unterstützung für Amazon EKS-Funktionen

Runtime Monitoring unterstützt Amazon EKS-Cluster, die auf Amazon EC2-Instances ausgeführt werden, und Amazon EKS Auto Mode.

Runtime Monitoring unterstützt keine Amazon EKS-Cluster mit Amazon EKS-Hybridknoten und solche, die darauf AWS Fargate laufen.

Informationen zu diesen Amazon EKS-Funktionen finden Sie unter Was ist Amazon EKS? im Amazon EKS-Benutzerhandbuch .

Validierung der architektonischen Anforderungen

Die von Ihnen verwendete Plattform kann sich darauf auswirken, wie der GuardDuty Security Agent den Empfang der Laufzeitereignisse von Ihren EKS-Clustern unterstützt GuardDuty . Sie müssen bestätigen, dass Sie eine der verifizierten Plattformen verwenden. Wenn Sie den GuardDuty Agenten manuell verwalten, stellen Sie sicher, dass die Kubernetes-Version die aktuell verwendete GuardDuty Agentenversion unterstützt.

Verifizierte Plattformen

Die Betriebssystemverteilung, die Kernelversion und die CPU-Architektur wirken sich auf die vom GuardDuty Security Agent bereitgestellte Unterstützung aus. Die Kernel-Unterstützung umfasste`BPF`, `Tracepoints` und`Kprobe`. Für CPU-Architekturen unterstützt Runtime Monitoring AMD64 (`x64`) und ARM64 (Graviton2 und höher). [1]

Die folgende Tabelle zeigt die verifizierte Konfiguration für die Bereitstellung des GuardDuty Security Agents und die Konfiguration von EKS Runtime Monitoring.

Verteilung des Betriebssystems [2]	Kernel-Version [3]	Unterstützte Kubernetes-Version
Flaschenrakete	5.4, 5,10, 5,15, 6,1 [4]	v1.23 - v1.36
Ubuntu	5.4, 5,10, 5,15, 6,1, 6,15, 6,16, 6,17, 6,18 [4]	v1.21 - v1.36

Verteilung des Betriebssystems [2]	Kernel-Version [3]	Unterstützte Kubernetes-Version
Amazon Linux 2	5.4, 5,10, 5,15, 6,1 [4]	v1.21 - v1.36
Amazon Linux 2023 [5]	5.4, 5,10, 5,15, 6,1, 6,8, 6,12 [4]	v1.21 - v1.36
RedHat 9.4	5,14 [4]	v1.21 - v1.36
Fedora 34	5,11, 5,17	v1.21 - v1.36
Fedora 40	6.8	v1.28 - v1.36
Fedora 41	6,12	V1.28 - V1.36
CentOS Stream 9	5,14	v1.21 - v1.36

1. Die Laufzeitüberwachung für Amazon EKS-Cluster unterstützt Graviton-Instances der ersten Generation wie A1-Instance-Typen nicht.
2. Unterstützung für verschiedene Betriebssysteme — GuardDuty hat die Runtime Monitoring-Unterstützung für die in der vorherigen Tabelle aufgeführte Betriebsdistribution verifiziert. Obwohl der GuardDuty Security Agent möglicherweise auf Betriebssystemen läuft, die in der vorherigen Tabelle nicht aufgeführt sind, kann das GuardDuty Team den erwarteten Sicherheitswert nicht garantieren.
3. Für jede Kernelversion müssen Sie das `CONFIG_DEBUG_INFO_BTF` Flag auf y (was wahr bedeutet) setzen. Dies ist erforderlich, damit der GuardDuty Security Agent wie erwartet ausgeführt werden kann.
4. Derzeit GuardDuty kann mit der Kernel-Version nichts generiert werden `6.1`[GuardDuty Findetypen für die Laufzeitüberwachung], mit dem etwas zu [DNS-Ereignisse (Domain Name System)] tun hat.
5. Runtime Monitoring unterstützt AL2023 mit der Veröffentlichung des GuardDuty Security Agents v1.6.0 und höher. Weitere Informationen finden Sie unter [GuardDuty Security Agent-Versionen für Amazon EKS-Ressourcen].

Kubernetes-Versionen, die vom Security Agent unterstützt werden GuardDuty

Die folgende Tabelle zeigt die Kubernetes-Versionen für Ihre EKS-Cluster, die vom Security Agent unterstützt werden. GuardDuty

Version des Amazon GuardDuty EKS-Zusatz-Sicherheitsagenten	Kubernetes-Version
v1.16.0 (aktuell - v1.16.0-eksbuild.2)	1,28 - 1,36
v1.15.0 (aktuell - v1.15.0-eksbuild.2)	1,28 - 1,36
v1.12.2 (aktuell - v1.12.2-eksbuild.2)	1,28 - 1,36
v1.12.1 (aktuell - v1.12.1-eksbuild.4)	1,28 - 1,35
v1.11.0 (aktuell - v1.11.0-eksbuild.4)	1,28 - 1,34
v1.10.0 (aktuell - v1.10.0-eksbuild.2)	1,21 - 1,33
v1.9.0 (aktuell - v1.9.0-eksbuild.2) v1.8.1 (aktuell - v1.8.1-eksbuild.2)	1,21 - 1,32
v1.7.1 v1.7.0 v1.6.1	1,21 - 1,31
v1.6.0 v1.5.0 v1.4.1 v1.4.0 v1.3.1	1,21 - 1,29
v1.3.0	1,21 - 1,28

Version des Amazon GuardDuty EKS-Zusatz-Sicherheitsagenten	Kubernetes-Version
v1.2.0	
v1.1.0	1,21 - 1,26
v1.0.0	1,21 - 1,25

Für einige Versionen des GuardDuty Security Agents wird der Standardsupport bald auslaufen.

Informationen zu den Agent-Release-Versionen finden Sie unterGuardDuty Security Agent-Versionen für Amazon EKS-Ressourcen.

CPU- und Arbeitsspeicherlimits

Die folgende Tabelle zeigt die CPU- und Speicherlimits für das Amazon EKS-Add-on für GuardDuty (`aws-guardduty-agent`).

Parameter	Minimale Grenze	Maximale Grenze
CPU	200m	1000m
Arbeitsspeicher	256 Mi	1024Mi

Wenn Sie das Amazon EKS-Add-On Version 1.5.0 oder höher verwenden, GuardDuty bietet es die Möglichkeit, das Add-On-Schema für Ihre CPU- und Speicherwerte zu konfigurieren. Informationen zum konfigurierbaren Bereich finden Sie unterKonfigurierbare Parameter und Werte.

Nachdem Sie die EKS-Laufzeit-Überwachung aktiviert und den Abdeckungsstatus Ihrer EKS-Cluster bewertet haben, können Sie die Container-Erkenntnis-Metriken einrichten und anzeigen. Weitere Informationen finden Sie unter Einrichten der CPU- und Arbeitsspeicherüberwachung.

Validierung der Service Control-Richtlinie Ihres Unternehmens

Wenn Sie eine Service Control Policy (SCP) zur Verwaltung von Berechtigungen in Ihrer Organisation eingerichtet haben, stellen Sie sicher, dass die Berechtigungsgrenze nicht einschränkend ist. `guardduty:SendSecurityTelemetry` GuardDuty benötigt diese Berechtigung, um die Laufzeitüberwachung für verschiedene Ressourcentypen zu unterstützen.

Wenn es sich bei Ihrem Konto um ein Mitgliedskonto handelt, wenden Sie sich an den entsprechenden delegierten Administrator. Informationen zur Verwaltung von SCPs für Ihre Organisation finden Sie unter Service Control Policies (SCPs).

Laufzeitüberwachung aktivieren GuardDuty

Bevor Sie Runtime Monitoring in Ihrem Konto aktivieren, stellen Sie sicher, dass der Ressourcentyp, für den Sie die Laufzeitereignisse überwachen möchten, die Plattformanforderungen unterstützt. Weitere Informationen finden Sie unter Voraussetzungen.

Wenn Sie EKS Runtime Monitoring vor dem Start von Runtime Monitoring verwendet haben, können Sie die APIs verwenden, um die vorhandene Konfiguration für EKS Runtime Monitoring zu überprüfen und zu aktualisieren. Sie können Ihre bestehende Konfiguration auch von EKS Runtime Monitoring zu Runtime Monitoring migrieren. Weitere Informationen finden Sie unter Migrieren von EKS Runtime Monitoring zu Runtime Monitoring.

> **Note**
>
> Derzeit enthält diese Dokumentation Schritte, um Runtime Monitoring für Ihre Konten und Ihr Unternehmen nur über die Konsole zu aktivieren. Sie können die Laufzeitüberwachung auch mithilfe von API-Aktionen oder AWS CLI für GuardDuty aktivieren.

Sie können die Laufzeitüberwachung mithilfe der Schritte in den folgenden Themen konfigurieren.

Inhalt

- Aktivierung von Runtime Monitoring für Umgebungen mit mehreren Konten
- Runtime Monitoring für ein eigenständiges Konto aktivieren

Aktivierung von Runtime Monitoring für Umgebungen mit mehreren Konten

In Umgebungen mit mehreren Konten kann nur das delegierte GuardDuty Administratorkonto die Laufzeitüberwachung für die Mitgliedskonten aktivieren oder deaktivieren und die automatische Agentenkonfiguration für die Ressourcentypen verwalten, die zu den Mitgliedskonten in ihrer Organisation gehören. Die GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Das Konto des delegierten GuardDuty Administratorkontos verwaltet ihre

Mitgliedskonten mithilfe von AWS Organizations. Weitere Informationen zu Umgebungen mit mehreren Konten finden Sie unter Verwaltung mehrerer Konten.

Für ein delegiertes Administratorkonto GuardDuty

Um Runtime Monitoring für ein delegiertes GuardDuty Administratorkonto zu aktivieren

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
3. Wählen Sie auf der Registerkarte Konfiguration im Konfigurationsabschnitt Runtime Monitoring die Option Bearbeiten aus.
4. Verwendung von Für alle Konten aktivieren

   Wenn Sie Runtime Monitoring für alle Konten aktivieren möchten, die zur Organisation gehören, einschließlich des delegierten GuardDuty Administratorkontos, wählen Sie „Für alle Konten aktivieren“.
5. Verwendung von Konten manuell konfigurieren

   Wenn Sie die Laufzeitüberwachung für jedes Mitgliedskonto einzeln aktivieren möchten, wählen Sie Konten manuell konfigurieren aus.

   - Wählen Sie im Abschnitt Delegierter Administrator (dieses Konto) die Option Aktivieren.
6. Verwalten Sie den Security Agent für Ihren Ressourcentyp. Weitere Informationen finden Sie unter Verwaltung der GuardDuty Sicherheitsagenten.

Für alle Mitgliedskonten

Um die Laufzeitüberwachung für alle Mitgliedskonten in der Organisation zu aktivieren

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Melden Sie sich mit dem delegierten GuardDuty Administratorkonto an.
2. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
3. Wählen Sie auf der Seite Runtime Monitoring auf der Registerkarte Konfiguration im Abschnitt Runtime Monitoring-Konfiguration die Option Bearbeiten aus.
4. Wählen Sie Für alle Konten aktivieren.

5. Verwalten Sie den Security Agent für Ihren Ressourcentyp. Weitere Informationen finden Sie unter Verwaltung der GuardDuty Sicherheitsagenten.

Für alle vorhandenen aktiven Mitgliedskonten

Um die Laufzeitüberwachung für bestehende Mitgliedskonten in der Organisation zu aktivieren

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Melden Sie sich mit dem delegierten GuardDuty Administratorkonto für die Organisation an.
2. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
3. Auf der Seite Runtime Monitoring können Sie auf der Registerkarte Konfiguration den aktuellen Status der Runtime Monitoring-Konfiguration einsehen.
4. Wählen Sie im Bereich Runtime Monitoring im Abschnitt Aktive Mitgliedskonten die Option Aktionen aus.
5. Wählen Sie im Dropdownmenü Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten.
6. Wählen Sie Bestätigen aus.
7. Verwalten Sie den Security Agent für Ihren Ressourcentyp. Weitere Informationen finden Sie unter Verwaltung der GuardDuty Sicherheitsagenten.

> **Note**
>
> Die Aktualisierung der Konfiguration der Mitgliedskonten kann bis zu 24 Stunden dauern.

Auto-enable Laufzeitüberwachung nur für neue Mitgliedskonten

Um die Laufzeitüberwachung für neue Mitgliedskonten in Ihrer Organisation zu aktivieren

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Melden Sie sich mit dem angegebenen delegierten GuardDuty Administratorkonto der Organisation an.
2. Wählen Sie im Navigationsbereich Runtime Monitoring

3. Wählen Sie auf der Registerkarte Konfiguration im Konfigurationsabschnitt Runtime Monitoring die Option Bearbeiten aus.
4. Wählen Sie Konten manuell konfigurieren.
5. Wählen Sie Automatisch für neue Mitgliedskonten aktivieren.
6. Verwalten Sie den Security Agent für Ihren Ressourcentyp. Weitere Informationen finden Sie unter Verwaltung der GuardDuty Sicherheitsagenten.

Nur für ausgewählte aktive Mitgliedskonten

Um die Laufzeitüberwachung für einzelne aktive Mitgliedskonten zu aktivieren

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Melden Sie sich mit den Anmeldedaten für das delegierte GuardDuty Administratorkonto an.
2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
3. Überprüfen Sie auf der Seite Konten die Werte in den Spalten Runtime Monitoring und Manage Agent automatisch. Diese Werte geben an, ob Runtime Monitoring und GuardDuty Agentenverwaltung für das entsprechende Konto aktiviert oder nicht aktiviert sind.
4. Wählen Sie in der Tabelle Konten das Konto aus, für das Sie Runtime Monitoring aktivieren möchten. Sie können mehrere Konten gleichzeitig auswählen.
5. Wählen Sie Bestätigen aus.
6. Wählen Sie Schutzpläne bearbeiten aus. Wählen Sie die geeignete Aktion aus.
7. Wählen Sie Bestätigen aus.
8. Verwalten Sie den Security Agent für Ihren Ressourcentyp. Weitere Informationen finden Sie unter Verwaltung der GuardDuty Sicherheitsagenten.

Runtime Monitoring für ein eigenständiges Konto aktivieren

Ein eigenständiges Konto besitzt die Entscheidung, ob ein Schutzplan AWS-Konto in einem bestimmten Bereich aktiviert oder deaktiviert werden soll AWS-Region.

Wenn Ihr Konto durch oder durch AWS Organizations die Einladungsmethode mit einem GuardDuty Administratorkonto verknüpft ist, gilt dieser Abschnitt nicht für Ihr Konto. Weitere Informationen finden Sie unter Aktivierung von Runtime Monitoring für Umgebungen mit mehreren Konten.

Nachdem Sie Runtime Monitoring aktiviert haben, stellen Sie sicher, dass der GuardDuty Security Agent durch automatische Konfiguration oder manuelle Bereitstellung installiert wird. Stellen Sie sicher, dass Sie den Security Agent installieren, um alle im folgenden Verfahren aufgeführten Schritte abzuschließen.

Um Runtime Monitoring in einem eigenständigen Konto zu aktivieren

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
3. Wählen Sie auf der Registerkarte „Konfiguration“ die Option „Aktivieren“, um die Laufzeitüberwachung für Ihr Konto zu aktivieren.
4. Verwalten Sie den Security Agent für Ihren Ressourcentyp. Weitere Informationen finden Sie unter Verwaltung der GuardDuty Sicherheitsagenten.

Verwaltung der GuardDuty Sicherheitsagenten

Sie können den GuardDuty Security Agent für die Ressource verwalten, die Sie überwachen möchten. Wenn Sie mehr als einen Ressourcentyp überwachen möchten, stellen Sie sicher, dass Sie den GuardDuty Agenten für diese Ressource verwalten.

Die folgenden Themen helfen Ihnen bei den nächsten Schritten zur Verwaltung des Security Agents.

Inhalt

- Aktivierung des automatisierten Sicherheitsagenten für die Amazon EC2-Instance
- Manuelles Verwalten des Security Agents für die Amazon EC2-Ressource
- Verwaltung des GuardDuty Sicherheitsagenten auf Bottlerocket (Amazon ECS auf Amazon EC2)
- Verwaltung des automatisierten Sicherheitsagenten für Fargate (nur Amazon ECS)
- Automatische Verwaltung des Security Agents für Amazon EKS-Ressourcen
- Manuelles Verwalten des Sicherheitsagenten für den Amazon EKS-Cluster
- Konfigurieren Sie die GuardDuty Security Agent-Parameter (Add-on) für Amazon EKS
- Validierung der VPC-Endpunktkonfiguration

Aktivierung des automatisierten Sicherheitsagenten für die Amazon EC2-Instance

Dieser Abschnitt enthält Schritte zur Aktivierung des GuardDuty automatisierten Agenten für Ihre Amazon EC2-Ressourcen in Ihrem eigenständigen Konto oder einer Umgebung mit mehreren Konten.

Bevor Sie fortfahren, stellen Sie sicher, dass Sie alle Anweisungen befolgen. Voraussetzungen für die Unterstützung von Amazon EC2-Instances

Themen

- Aktivierung GuardDuty des Agenten für Amazon EC2-Ressourcen in einer Umgebung mit mehreren Konten
- Aktivierung des GuardDuty automatisierten Agenten für Amazon EC2-Ressourcen in einem eigenständigen Konto
- Migration vom manuellen Amazon EC2-Agenten zum automatisierten Agenten

Wenn Sie von der manuellen Verwaltung des GuardDuty Agenten zur Aktivierung des GuardDuty automatisierten Agenten migrieren, finden Migration vom manuellen Amazon EC2-Agenten zum automatisierten Agenten Sie unter, bevor Sie die Schritte zur Aktivierung des GuardDuty automatisierten Agenten ausführen.

Aktivierung GuardDuty des Agenten für Amazon EC2-Ressourcen in einer Umgebung mit mehreren Konten

In einer Umgebung mit mehreren Konten kann nur das delegierte GuardDuty Administratorkonto die automatische Agentenkonfiguration für die Ressourcentypen aktivieren oder deaktivieren, die zu den Mitgliedskonten in ihrer Organisation gehören. Die GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Das delegierte GuardDuty Administratorkonto verwaltet ihre Mitgliedskonten mithilfe von AWS Organizations. Weitere Informationen zu Umgebungen mit mehreren Konten finden Sie unter Verwaltung mehrerer Konten.

Für ein delegiertes Administratorkonto GuardDuty

Configure for all instances

> Wenn Sie für Runtime Monitoring die Option Für alle Konten aktivieren ausgewählt haben, wählen Sie eine der folgenden Optionen für das delegierte GuardDuty Administratorkonto:

- Option 1

  Wählen Sie unter Automatisierte Agentenkonfiguration im Abschnitt EC2 die Option Für alle Konten aktivieren aus.

- Option 2
  - Wählen Sie unter Automatisierte Agentenkonfiguration im Abschnitt EC2 die Option Konten manuell konfigurieren aus.
  - Wählen Sie unter Delegated Administrator (dieses Konto) die Option Aktivieren aus.
- Wählen Sie Speichern.

Wenn Sie „Konten manuell für Runtime Monitoring konfigurieren“ ausgewählt haben, gehen Sie wie folgt vor:

- Wählen Sie unter Automatisierte Agentenkonfiguration im Abschnitt EC2 die Option Konten manuell konfigurieren aus.
- Wählen Sie unter Delegated Administrator (dieses Konto) die Option Aktivieren aus.
- Wählen Sie Speichern.

Unabhängig davon, welche Option Sie wählen, um die automatische Agent-Konfiguration für ein delegiertes GuardDuty Administratorkonto zu aktivieren, können Sie überprüfen, ob die SSM-Verknüpfung, die GuardDuty erstellt wird, den Security Agent auf allen EC2-Ressourcen installiert und verwaltet, die zu diesem Konto gehören.

1. Öffnen Sie die Konsole unter AWS Systems Manager . https://console.aws.amazon.com/systems-manager/
2. Öffnen Sie die Registerkarte Ziele für die SSM-Zuordnung (`GuardDutyRuntimeMonitoring-do-not-delete`). Beachten Sie, dass der Tag-Schlüssel als InstanceIds angezeigt wird.

Using inclusion tag in selected instances

Um den GuardDuty Agenten für ausgewählte Amazon EC2-Instances zu konfigurieren

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon EC2-Konsole unter. https://console.aws.amazon.com/ec2/

2. Fügen Sie den Instanzen, die Sie überwachen und potenzielle Bedrohungen erkennen GuardDuty möchten, das `true` Tag`GuardDutyManaged`: hinzu. Informationen zum Hinzufügen dieses Tags finden Sie unter So fügen Sie einer einzelnen Ressource ein Tag hinzu.

   Durch Hinzufügen dieses Tags GuardDuty kann der Security Agent für diese ausgewählten EC2-Instances installiert und verwaltet werden. Sie müssen die automatische Agentenkonfiguration nicht explizit aktivieren.

3. Sie können überprüfen, ob die SSM-Zuordnung, die GuardDuty erstellt wird, den Security Agent nur auf den EC2-Ressourcen installiert und verwaltet, die mit den Inklusion-Tags gekennzeichnet sind.

   Öffnen Sie die AWS Systems Manager Konsole unter. https://console.aws.amazon.com/systems-manager/

   - Öffnen Sie die Registerkarte Ziele für die SSM-Zuordnung, die erstellt wird (`GuardDutyRuntimeMonitoring-do-not-delete`). Der Tag-Schlüssel wird als Tag: GuardDutyManaged angezeigt.

Using exclusion tag in selected instances

> **Note**
>
> Stellen Sie sicher, dass Sie Ihren Amazon EC2-Instances das Ausschluss-Tag hinzufügen, bevor Sie sie starten. Sobald Sie die automatische Agentenkonfiguration für Amazon EC2 aktiviert haben, fällt jede EC2-Instance, die ohne Ausschluss-Tag gestartet wird, unter die GuardDuty automatische Agentenkonfiguration.

Um den GuardDuty Agenten für ausgewählte Amazon EC2-Instances zu konfigurieren

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon EC2-Konsole unter. https://console.aws.amazon.com/ec2/
2. Fügen Sie den Instances, die Sie nicht überwachen und potenzielle Bedrohungen erkennen GuardDuty möchten, das `false` Tag`GuardDutyManaged`: hinzu. Informationen zum Hinzufügen dieses Tags finden Sie unter So fügen Sie einer einzelnen Ressource ein Tag hinzu.

3. Für den Ausschluss-Tags müssen verfügbar sein Führen Sie in den Instanz-Metadaten die folgenden Schritte aus:

   a. Sehen Sie sich auf der Registerkarte „Details“ Ihrer Instanz den Status für „Tags zulassen“ in Instanz-Metadaten an.

      Wenn sie derzeit deaktiviert ist, führen Sie die folgenden Schritte aus, um den Status in Aktiviert zu ändern. Andernfalls überspringen Sie diesen Schritt.

   b. Wählen Sie im Menü Aktionen die Option Instanzeinstellungen aus.

   c. Wählen Sie „Tags in Instanz-Metadaten zulassen“.

4. Nachdem Sie das Ausschluss-Tag hinzugefügt haben, führen Sie dieselben Schritte aus, die auf der Registerkarte „Für alle Instanzen konfigurieren“ angegeben sind.

Sie können jetzt die Laufzeit beurteilenLaufzeitabdeckung und Problembehandlung für die Amazon EC2-Instance.

Auto-enable für alle Mitgliedskonten

> **Note**
>
> Die Aktualisierung der Konfiguration der Mitgliedskonten kann bis zu 24 Stunden dauern.

Configure for all instances

Bei den folgenden Schritten wird davon ausgegangen, dass Sie im Abschnitt Runtime Monitoring die Option Für alle Konten aktivieren ausgewählt haben:

1. Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration für Amazon EC2 die Option Für alle Konten aktivieren aus.
2. Sie können überprüfen, ob die SSM-Zuordnung, die GuardDuty erstellt (`GuardDutyRuntimeMonitoring-do-not-delete`), den Security Agent auf allen EC2-Ressourcen installiert und verwaltet, die zu diesem Konto gehören.

   a. Öffnen Sie die AWS Systems Manager Konsole unter. https://console.aws.amazon.com/systems-manager/

   b. Öffnen Sie die Registerkarte Ziele für die SSM-Zuordnung. Beachten Sie, dass der Tag-Schlüssel als InstanceIds angezeigt wird.

Using inclusion tag in selected instances

Um den GuardDuty Agenten für ausgewählte Amazon EC2-Instances zu konfigurieren

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon EC2-Konsole unter. https://console.aws.amazon.com/ec2/
2. Fügen Sie den EC2-Instances, die Sie überwachen und potenzielle Bedrohungen erkennen GuardDuty möchten, das `true` Tag`GuardDutyManaged`: hinzu. Informationen zum Hinzufügen dieses Tags finden Sie unter So fügen Sie einer einzelnen Ressource ein Tag hinzu.

   Durch Hinzufügen dieses Tags GuardDuty kann der Security Agent für diese ausgewählten EC2-Instances installiert und verwaltet werden. Sie müssen die automatische Agentenkonfiguration nicht explizit aktivieren.
3. Sie können überprüfen, ob die SSM-Zuordnung, die GuardDuty erstellt wird, den Security Agent auf allen EC2-Ressourcen installiert und verwaltet, die zu Ihrem Konto gehören.

   a. Öffnen Sie die AWS Systems Manager Konsole unter. https://console.aws.amazon.com/systems-manager/

   b. Öffnen Sie die Registerkarte Ziele für die SSM-Zuordnung (`GuardDutyRuntimeMonitoring-do-not-delete`). Beachten Sie, dass der Tag-Schlüssel als InstanceIds angezeigt wird.

Using exclusion tag in selected instances

> **Note**
>
> Stellen Sie sicher, dass Sie Ihren Amazon EC2-Instances das Ausschluss-Tag hinzufügen, bevor Sie sie starten. Sobald Sie die automatische Agentenkonfiguration für Amazon EC2 aktiviert haben, fällt jede EC2-Instance, die ohne Ausschluss-Tag gestartet wird, unter die GuardDuty automatische Agentenkonfiguration.

Um den GuardDuty Security Agent für ausgewählte Amazon EC2-Instances zu konfigurieren

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon EC2-Konsole unter. https://console.aws.amazon.com/ec2/

2. Fügen Sie den Instances, die Sie nicht überwachen und potenzielle Bedrohungen erkennen GuardDuty möchten, das `false` Tag`GuardDutyManaged`: hinzu. Informationen zum Hinzufügen dieses Tags finden Sie unter So fügen Sie einer einzelnen Ressource ein Tag hinzu.
3. Für den Ausschluss-Tags müssen verfügbar sein Führen Sie in den Instanz-Metadaten die folgenden Schritte aus:

   a. Sehen Sie sich auf der Registerkarte „Details“ Ihrer Instanz den Status für „Tags zulassen“ in Instanz-Metadaten an.

      Wenn sie derzeit deaktiviert ist, führen Sie die folgenden Schritte aus, um den Status in Aktiviert zu ändern. Andernfalls überspringen Sie diesen Schritt.

   b. Wählen Sie im Menü Aktionen die Option Instanzeinstellungen aus.

   c. Wählen Sie „Tags in Instanz-Metadaten zulassen“.
4. Nachdem Sie das Ausschluss-Tag hinzugefügt haben, führen Sie dieselben Schritte aus, die auf der Registerkarte „Für alle Instanzen konfigurieren“ angegeben sind.

Sie können jetzt die Laufzeit beurteilenLaufzeitabdeckung und Problembehandlung für die Amazon EC2-Instance.

Auto-enable nur für neue Mitgliedskonten

Das delegierte GuardDuty Administratorkonto kann die automatische Agentenkonfiguration für die Amazon EC2-Ressource so einrichten, dass sie automatisch für die neuen Mitgliedskonten aktiviert wird, wenn sie der Organisation beitreten.

Configure for all instances

Bei den folgenden Schritten wird davon ausgegangen, dass Sie im Abschnitt Runtime Monitoring die Option Automatisch für neue Mitgliedskonten aktivieren ausgewählt haben:

1. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
2. Wählen Sie auf der Seite Runtime Monitoring die Option Bearbeiten aus.
3. Wählen Sie Automatisch für neue Mitgliedskonten aktivieren. Dieser Schritt stellt sicher, dass jedes Mal, wenn ein neues Konto Ihrer Organisation beitritt, die automatische Agentenkonfiguration für Amazon EC2 automatisch für das entsprechende Konto aktiviert wird. Nur das delegierte GuardDuty Administratorkonto der Organisation kann diese Auswahl ändern.

4. Wählen Sie Speichern.

Wenn ein neues Mitgliedskonto der Organisation beitritt, wird diese Konfiguration für dieses Mitglied automatisch aktiviert. GuardDuty Um den Security Agent für die Amazon EC2-Instances zu verwalten, die zu diesem neuen Mitgliedskonto gehören, stellen Sie sicher, dass alle Voraussetzungen erfüllt Für die EC2-Instanz sind.

Wenn eine SSM-Zuordnung erstellt wird (`GuardDutyRuntimeMonitoring-do-not-delete`), können Sie überprüfen, ob die SSM-Zuordnung den Security Agent auf allen EC2-Instances installiert und verwaltet, die zum neuen Mitgliedskonto gehören.

- Öffnen Sie die Konsole unter AWS Systems Manager . https://console.aws.amazon.com/systems-manager/
- Öffnen Sie die Registerkarte Ziele für die SSM-Zuordnung. Beachten Sie, dass der Tag-Schlüssel als InstanceIds angezeigt wird.

Using inclusion tag in selected instances

Um den GuardDuty Security Agent für ausgewählte Instanzen in Ihrem Konto zu konfigurieren

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Fügen Sie den Instances, die Sie überwachen und potenzielle Bedrohungen erkennen GuardDuty möchten, das `true` Tag`GuardDutyManaged`: hinzu. Informationen zum Hinzufügen dieses Tags finden Sie unter So fügen Sie einer einzelnen Ressource ein Tag hinzu.

   Wenn Sie dieses Tag hinzufügen GuardDuty , können Sie den Security Agent für diese ausgewählten Instanzen installieren und verwalten. Sie müssen die automatische Agentenkonfiguration nicht explizit aktivieren.
3. Sie können überprüfen, ob die SSM-Zuordnung, die GuardDuty erstellt wird, den Security Agent nur auf den EC2-Ressourcen installiert und verwaltet, die mit den Inklusion-Tags gekennzeichnet sind.

   a. Öffnen Sie die AWS Systems Manager Konsole unter. https://console.aws.amazon.com/systems-manager/

b. Öffnen Sie die Registerkarte Ziele für die SSM-Zuordnung, die erstellt wird. Der Tag-Schlüssel wird als Tag: GuardDutyManaged angezeigt.

Using exclusion tag in selected instances

> **Note**
>
> Stellen Sie sicher, dass Sie Ihren Amazon EC2-Instances das Ausschluss-Tag hinzufügen, bevor Sie sie starten. Sobald Sie die automatische Agentenkonfiguration für Amazon EC2 aktiviert haben, fällt jede EC2-Instance, die ohne Ausschluss-Tag gestartet wird, unter die GuardDuty automatische Agentenkonfiguration.

Um den GuardDuty Security Agent für bestimmte Instances in Ihrem eigenständigen Konto zu konfigurieren

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Fügen Sie den Instances, die Sie nicht überwachen und potenzielle Bedrohungen erkennen GuardDuty möchten, das `false` Tag`GuardDutyManaged`: hinzu. Informationen zum Hinzufügen dieses Tags finden Sie unter So fügen Sie einer einzelnen Ressource ein Tag hinzu.
3. Für den Ausschluss-Tags müssen verfügbar sein Führen Sie in den Instanz-Metadaten die folgenden Schritte aus:

   a. Sehen Sie sich auf der Registerkarte „Details“ Ihrer Instanz den Status für „Tags zulassen“ in Instanz-Metadaten an.

      Wenn sie derzeit deaktiviert ist, führen Sie die folgenden Schritte aus, um den Status in Aktiviert zu ändern. Andernfalls überspringen Sie diesen Schritt.

   b. Wählen Sie im Menü Aktionen die Option Instanzeinstellungen aus.

   c. Wählen Sie „Tags in Instanz-Metadaten zulassen“.

4. Nachdem Sie das Ausschluss-Tag hinzugefügt haben, führen Sie dieselben Schritte aus, die auf der Registerkarte „Für alle Instanzen konfigurieren“ angegeben sind.

Sie können jetzt die Laufzeit beurteilenLaufzeitabdeckung und Problembehandlung für die Amazon EC2-Instance.

Nur ausgewählte Mitgliedskonten

Configure for all instances

1. Wählen Sie auf der Seite Konten ein oder mehrere Konten aus, für die Sie die Runtime Monitoring-Automated Agent-Konfiguration (Amazon EC2) aktivieren möchten. Stellen Sie sicher, dass für die Konten, die Sie in diesem Schritt auswählen, Runtime Monitoring bereits aktiviert ist.
2. Wählen Sie unter Schutzpläne bearbeiten die entsprechende Option aus, um die Runtime Monitoring-Automated Agent-Konfiguration (Amazon EC2) zu aktivieren.
3. Wählen Sie Bestätigen aus.

Using inclusion tag in selected instances

Um den GuardDuty Security Agent für ausgewählte Instances zu konfigurieren

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Fügen Sie den Instances, die Sie überwachen und potenzielle Bedrohungen erkennen GuardDuty möchten, das `true` Tag`GuardDutyManaged`: hinzu. Informationen zum Hinzufügen dieses Tags finden Sie unter So fügen Sie einer einzelnen Ressource ein Tag hinzu.

   Wenn Sie dieses Tag hinzufügen GuardDuty , können Sie den Security Agent für Ihre markierten Amazon EC2-Instances verwalten. Sie müssen die automatische Agentenkonfiguration nicht explizit aktivieren (Runtime Monitoring — Automated Agent Configuration (EC2)).

Using exclusion tag in selected instances

> **Note**
>
> Stellen Sie sicher, dass Sie Ihren Amazon EC2-Instances das Ausschluss-Tag hinzufügen, bevor Sie sie starten. Sobald Sie die automatische Agentenkonfiguration für

Amazon EC2 aktiviert haben, fällt jede EC2-Instance, die ohne Ausschluss-Tag gestartet wird, unter die GuardDuty automatische Agentenkonfiguration.

Um den GuardDuty Security Agent für ausgewählte Instances zu konfigurieren

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Fügen Sie den EC2-Instances, die Sie nicht überwachen oder potenzielle Bedrohungen erkennen GuardDuty möchten, das `false` `TagGuardDutyManaged`: hinzu. Informationen zum Hinzufügen dieses Tags finden Sie unter So fügen Sie einer einzelnen Ressource ein Tag hinzu.
3. Für den Ausschluss-Tags müssen verfügbar sein Führen Sie in den Instanz-Metadaten die folgenden Schritte aus:

   a. Sehen Sie sich auf der Registerkarte „Details“ Ihrer Instanz den Status für „Tags zulassen“ in Instanz-Metadaten an.

      Wenn sie derzeit deaktiviert ist, führen Sie die folgenden Schritte aus, um den Status in Aktiviert zu ändern. Andernfalls überspringen Sie diesen Schritt.

   b. Wählen Sie im Menü Aktionen die Option Instanzeinstellungen aus.

   c. Wählen Sie „Tags in Instanz-Metadaten zulassen“.
4. Nachdem Sie das Ausschluss-Tag hinzugefügt haben, führen Sie dieselben Schritte aus, die auf der Registerkarte „Für alle Instanzen konfigurieren“ angegeben sind.

Sie können es jetzt beurteilenLaufzeitabdeckung und Problembehandlung für die Amazon EC2-Instance.

Aktivierung des GuardDuty automatisierten Agenten für Amazon EC2-Ressourcen in einem eigenständigen Konto

Ein eigenständiges Konto besitzt die Entscheidung, ob ein Schutzplan AWS-Konto in einem bestimmten Bereich aktiviert oder deaktiviert werden soll AWS-Region.

Wenn Ihr Konto durch oder durch AWS Organizations die Einladungsmethode mit einem GuardDuty Administratorkonto verknüpft ist, gilt dieser Abschnitt nicht für Ihr Konto. Weitere Informationen finden Sie unter Aktivierung von Runtime Monitoring für Umgebungen mit mehreren Konten.

Nachdem Sie Runtime Monitoring aktiviert haben, stellen Sie sicher, dass der GuardDuty Security Agent durch automatische Konfiguration oder manuelle Bereitstellung installiert wird. Stellen Sie sicher, dass Sie den Security Agent installieren, um alle im folgenden Verfahren aufgeführten Schritte abzuschließen.

Wählen Sie je nach Ihrer Präferenz, alle oder ausgewählte Amazon EC2-Ressourcen zu überwachen, eine bevorzugte Methode aus und folgen Sie den Schritten in der folgenden Tabelle.

Configure for all instances

Um Runtime Monitoring für alle Instances in Ihrem eigenständigen Konto zu konfigurieren

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
3. Wählen Sie auf der Registerkarte Konfiguration die Option Bearbeiten aus.
4. Wählen Sie im Abschnitt EC2 die Option Enable aus.
5. Wählen Sie Speichern.
6. Sie können überprüfen, ob die SSM-Zuordnung, die GuardDuty erstellt wird, den Security Agent auf allen EC2-Ressourcen installiert und verwaltet, die zu Ihrem Konto gehören.
   a. Öffnen Sie die AWS Systems Manager Konsole unter. https://console.aws.amazon.com/systems-manager/
   b. Öffnen Sie die Registerkarte Ziele für die SSM-Zuordnung (`GuardDutyRuntimeMonitoring-do-not-delete`). Beachten Sie, dass der Tag-Schlüssel als InstanceIds angezeigt wird.

Using inclusion tag in selected instances

Um den GuardDuty Security Agent für ausgewählte Amazon EC2-Instances zu konfigurieren

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon EC2-Konsole unter. https://console.aws.amazon.com/ec2/
2. Fügen Sie den Instances, die Sie überwachen und potenzielle Bedrohungen erkennen GuardDuty möchten, das `true` Tag`GuardDutyManaged`: hinzu. Informationen zum Hinzufügen dieses Tags finden Sie unter So fügen Sie einer einzelnen Ressource ein Tag hinzu.

3. Sie können überprüfen, ob die SSM-Zuordnung, die GuardDuty erstellt wird, den Security Agent nur auf den EC2-Ressourcen installiert und verwaltet, die mit den Inklusion-Tags gekennzeichnet sind.

   Öffnen Sie die AWS Systems Manager Konsole unter. https://console.aws.amazon.com/systems-manager/

   - Öffnen Sie die Registerkarte Ziele für die SSM-Zuordnung, die erstellt wird (`GuardDutyRuntimeMonitoring-do-not-delete`). Der Tag-Schlüssel wird als Tag: GuardDutyManaged angezeigt.

Using exclusion tag in selected instances

> **Note**
>
> Stellen Sie sicher, dass Sie Ihren Amazon EC2-Instances das Ausschluss-Tag hinzufügen, bevor Sie sie starten. Sobald Sie die automatische Agentenkonfiguration für Amazon EC2 aktiviert haben, fällt jede EC2-Instance, die ohne Ausschluss-Tag gestartet wird, unter die GuardDuty automatische Agentenkonfiguration.

Um den GuardDuty Security Agent für ausgewählte Amazon EC2-Instances zu konfigurieren

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon EC2-Konsole unter. https://console.aws.amazon.com/ec2/
2. Fügen Sie den Instances, die Sie nicht überwachen und potenzielle Bedrohungen erkennen GuardDuty möchten, das `false` Tag`GuardDutyManaged`: hinzu. Informationen zum Hinzufügen dieses Tags finden Sie unter So fügen Sie einer einzelnen Ressource ein Tag hinzu.
3. Für den Ausschluss-Tags müssen verfügbar sein Führen Sie in den Instanz-Metadaten die folgenden Schritte aus:

   a. Sehen Sie sich auf der Registerkarte „Details“ Ihrer Instanz den Status für „Tags zulassen“ in Instanz-Metadaten an.

      Wenn sie derzeit deaktiviert ist, führen Sie die folgenden Schritte aus, um den Status in Aktiviert zu ändern. Andernfalls überspringen Sie diesen Schritt.

   b. Wählen Sie die Instanz aus, für die Sie Tags zulassen möchten.

c. Wählen Sie im Menü Aktionen die Option Instanzeinstellungen aus.

d. Wählen Sie „Tags in Instanz-Metadaten zulassen“.

e. Wählen Sie unter Zugriff auf Tags in Instanzmetadaten die Option Zulassen aus.

f. Wählen Sie Speichern.

4. Nachdem Sie das Ausschluss-Tag hinzugefügt haben, führen Sie dieselben Schritte aus, die auf der Registerkarte „Für alle Instanzen konfigurieren“ angegeben sind.

Sie können jetzt die Laufzeit beurteilen. Laufzeitabdeckung und Problembehandlung für die Amazon EC2-Instance

Migration vom manuellen Amazon EC2-Agenten zum automatisierten Agenten

Dieser Abschnitt gilt für Sie, AWS-Konto wenn Sie den Security Agent zuvor manuell verwaltet haben und nun die GuardDuty automatisierte Agentenkonfiguration verwenden möchten. Wenn dies nicht auf Sie zutrifft, fahren Sie mit der Konfiguration des Security Agents für Ihr Konto fort.

Wenn Sie den GuardDuty automatisierten Agenten aktivieren, GuardDuty verwaltet er den Security Agent in Ihrem Namen. Informationen darüber, welche Schritte unternommen werden, finden GuardDuty Sie unterVerwenden Sie die automatische Agentenkonfiguration (empfohlen).

Bereinigen von Ressourcen

Löschen Sie die SSM-Zuordnung

- Löschen Sie alle SSM-Verknüpfungen, die Sie möglicherweise erstellt haben, als Sie den Security Agent für Amazon EC2 manuell verwaltet haben. Weitere Informationen finden Sie unter Verknüpfungen löschen.
- Dies geschieht, damit das Unternehmen die Verwaltung von SSM-Aktionen übernehmen GuardDuty kann, unabhängig davon, ob Sie automatisierte Agenten auf Konto- oder Instanzebene verwenden (mithilfe von Einschluss- oder Ausschluss-Tags). Weitere Informationen darüber, welche SSM-Aktionen ausführen können, GuardDuty finden Sie unter. Service-linked Rollenberechtigungen für GuardDuty
- Wenn Sie eine SSM-Zuordnung löschen, die zuvor für die manuelle Verwaltung des Security Agents erstellt wurde, kann es bei GuardDuty der automatischen Erstellung einer SSM-Zuordnung zur Verwaltung des Security Agents zu einer kurzen Überschneidung kommen. Während dieses Zeitraums kann es aufgrund der SSM-Planung zu Konflikten kommen. Weitere Informationen finden Sie unter Amazon EC2 SSM-Planung.

Verwalten Sie Inklusions- und Ausschluss-Tags für Ihre Amazon EC2-Instances

- Einschluss-Tags — Wenn Sie die GuardDuty automatische Agentenkonfiguration nicht aktivieren, aber eine Ihrer Amazon EC2-Instances mit einem Einschluss-Tag (`GuardDutyManaged:true`) kennzeichnen, wird eine SSM-Verknüpfung GuardDuty erstellt, die den Security Agent auf den ausgewählten EC2-Instances installiert und verwaltet. Dies ist ein erwartetes Verhalten, das Ihnen bei der Verwaltung des Security Agents nur auf ausgewählten EC2-Instances hilft. Weitere Informationen finden Sie unter So funktioniert Runtime Monitoring mit Amazon EC2-Instances.

  Um zu GuardDuty verhindern, dass der Security Agent installiert und verwaltet wird, entfernen Sie das Inklusion-Tag von diesen EC2-Instances. Weitere Informationen finden Sie unter Hinzufügen und Löschen von Tags im Amazon EC2-Benutzerhandbuch.
- Ausschluss-Tags — Wenn Sie die GuardDuty automatische Agentenkonfiguration für alle EC2-Instances in Ihrem Konto aktivieren möchten, stellen Sie sicher, dass keine EC2-Instance mit einem Ausschluss-Tag (:) `GuardDutyManaged` gekennzeichnet ist. `false`

Manuelles Verwalten des Security Agents für die Amazon EC2-Ressource

Dieser Abschnitt enthält die Schritte zur manuellen Installation und Aktualisierung des Security Agents für Ihre Amazon EC2-Ressourcen.

Nachdem Sie Runtime Monitoring aktiviert haben, müssen Sie den GuardDuty Security Agent manuell installieren. Um den GuardDuty Security Agent manuell zu verwalten, müssen Sie zunächst manuell einen Amazon VPC-Endpunkt erstellen. Danach können Sie den Security Agent so installieren, dass er GuardDuty die Laufzeitereignisse von den Amazon EC2-Instances empfängt. Wenn eine neue Agentenversion für diese Ressource GuardDuty veröffentlicht wird, können Sie die Agentenversion in Ihrem Konto aktualisieren.

Die folgenden Themen enthalten die Schritte zur kontinuierlichen Verwaltung des Security Agents für Ihre Amazon EC2-Ressourcen.

Themen

- Voraussetzung — Manuelles Erstellen des Amazon VPC-Endpunkts
- Manuelles Installieren des Security Agents
- Manuelles Aktualisieren des GuardDuty Security Agents für die Amazon EC2-Instance

Voraussetzung — Manuelles Erstellen des Amazon VPC-Endpunkts

Bevor Sie den GuardDuty Security Agent installieren können, müssen Sie einen Amazon Virtual Private Cloud (Amazon VPC) -Endpunkt erstellen. Dies hilft dabei, die Laufzeitereignisse Ihrer Amazon EC2-Instances zu GuardDuty empfangen.

> **Note**
>
> Für die Nutzung des VPC-Endpunkts fallen keine zusätzlichen Kosten an.

Um einen Amazon VPC-Endpunkt zu erstellen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon VPC-Konsole unter. https://console.aws.amazon.com/vpc/
2. Wählen Sie im Navigationsbereich unter VPC Private Cloud die Option Endpoints aus.
3. Klicken Sie auf Endpunkt erstellen.
4. Wählen Sie auf der Seite Endpunkt erstellen für Servicekategorie die Option Andere Endpunkt-Services.
5. Geben Sie unter Servicename **`com.amazonaws.`*`us-east-1`*`.guardduty-data`** ein.

   Stellen Sie sicher, dass Sie durch Ihre *`us-east-1`* ersetzen. AWS-Region Dies muss dieselbe Region sein wie die Amazon EC2-Instance, die zu Ihrer AWS Konto-ID gehört.
6. Wählen Sie Service verifizieren.
7. Nachdem der Dienstname erfolgreich verifiziert wurde, wählen Sie die VPC aus, in der sich Ihre Instance befindet. Fügen Sie die folgende Richtlinie hinzu, um die Nutzung von Amazon VPC-Endpunkten nur auf das angegebene Konto zu beschränken. Unter Angabe der unter dieser Richtlinie angegebenen Organisations-`Condition` können Sie die folgende Richtlinie aktualisieren, um den Zugriff auf Ihren Endpunkt einzuschränken. Informationen zur Bereitstellung der Amazon VPC-Endpunktunterstützung für bestimmte Konto-IDs in Ihrer Organisation finden Sie unter. Organization condition to restrict access to your endpoint

   JSON

```
{
 "Version":"2012-10-17",
 "Statement": [
```

```
  {
   "Action": "*",
   "Resource": "*",
   "Effect": "Allow",
   "Principal": "*"
  },
  {
   "Condition": {
    "StringNotEquals": {
     "aws:PrincipalAccount": "111122223333"
    }
   },
   "Action": "*",
   "Resource": "*",
   "Effect": "Deny",
   "Principal": "*"
  }
 ]
}
```

Die `aws:PrincipalAccount`-Konto-ID muss mit dem Konto übereinstimmen, das die VPC und den VPC-Endpunkt enthält. Die folgende Liste zeigt, wie Sie den VPC-Endpunkt mit anderen AWS Konto-IDs teilen können:

- Um mehrere Konten für den Zugriff auf den VPC-Endpunkt anzugeben, `"aws:PrincipalAccount: "111122223333"` ersetzen Sie ihn durch den folgenden Block:

  ```
  "aws:PrincipalAccount": [
           "666666666666",
           "555555555555"
       ]
  ```

  Stellen Sie sicher, dass Sie die AWS Konto-IDs durch die Konto-IDs der Konten ersetzen, die auf den VPC-Endpunkt zugreifen müssen.

- Um allen Mitgliedern einer Organisation den Zugriff auf den VPC-Endpunkt zu ermöglichen, `"aws:PrincipalAccount: "111122223333"` ersetzen Sie diese durch die folgende Zeile:

  ```
  "aws:PrincipalOrgID": "o-abcdef0123"
  ```

Stellen Sie sicher, dass Sie die Organisation *o-abcdef0123* durch Ihre Organisations-ID ersetzen.

- Um den Zugriff auf eine Ressource anhand einer Organisations-ID einzuschränken, fügen Sie Ihre `ResourceOrgID` zur Richtlinie hinzu. Weitere Informationen finden Sie unter `aws:ResourceOrgID` im IAM-Benutzerhandbuch.

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. Wählen Sie unter Zusätzliche Einstellungen die Option DNS-Name aktivieren.
9. Wählen Sie unter Subnetze die Subnetze aus, in denen sich Ihre Instance befindet.
10. Wählen Sie unter Sicherheitsgruppen eine Sicherheitsgruppe aus, für die der eingehende Port 443 von Ihrer VPC (oder Ihrer Amazon EC2-Instance) aus aktiviert ist. Wenn Sie noch keine Sicherheitsgruppe haben, für die ein eingehender Port 443 aktiviert ist, finden Sie weitere Informationen unter Erstellen einer Sicherheitsgruppe für Ihre VPC im Amazon VPC-Benutzerhandbuch.

    Wenn beim Einschränken der eingehenden Berechtigungen für Ihre VPC (oder Instance) ein Problem auftritt, können Sie den eingehenden 443-Port von einer beliebigen IP-Adresse aus verwenden. (`0.0.0.0/0`) Es wird jedoch GuardDuty empfohlen, IP-Adressen zu verwenden, die dem CIDR-Block für Ihre VPC entsprechen. Weitere Informationen finden Sie unter VPC-CIDR-Blöcke im Amazon VPC-Benutzerhandbuch.

Nachdem Sie die Schritte befolgt haben, finden Sie unter Validierung der VPC-Endpunktkonfiguration Um sicherzustellen, dass der VPC-Endpunkt korrekt eingerichtet wurde.

Manuelles Installieren des Security Agents

GuardDuty bietet die folgenden zwei Methoden zur Installation des GuardDuty Security Agents auf Ihren Amazon EC2-Instances. Bevor Sie fortfahren, stellen Sie sicher, dass Sie die Schritte unter Voraussetzung — Manuelles Erstellen des Amazon VPC-Endpunkts befolgen.

Wählen Sie eine bevorzugte Zugriffsmethode, um den Security Agent in Ihren Amazon EC2-Ressourcen zu installieren.

- Methode 1 — Verwenden AWS Systems Manager— Für diese Methode muss Ihre Amazon EC2-Instance verwaltet werden AWS Systems Manager .

- Methode 2: Verwenden von Linux-Paketmanagern— Sie können diese Methode verwenden, unabhängig davon, ob Ihre Amazon EC2-Instances verwaltet werden AWS Systems Manager oder nicht. Basierend auf Ihren Betriebssystemverteilungen können Sie eine geeignete Methode wählen, um entweder RPM-Skripte oder Debian-Skripte zu installieren. Wenn Sie die Fedora-Plattform verwenden, müssen Sie diese Methode verwenden, um den Agenten zu installieren.

Methode 1 — Verwenden AWS Systems Manager

Um diese Methode zu verwenden, stellen Sie sicher, dass Ihre Amazon EC2-Instances AWS Systems Manager verwaltet werden, und installieren Sie dann den Agenten.

AWS Systems Manager verwaltete Amazon EC2-Instanz

Gehen Sie wie folgt vor, um Ihre Amazon EC2-Instances AWS Systems Manager zu verwalten.

- AWS Systems Managerhilft Ihnen dabei, Ihre AWS Anwendungen und Ressourcen durchgängig zu verwalten und sichere Abläufe in großem Maßstab zu ermöglichen.

  Informationen zur Verwaltung Ihrer Amazon EC2-Instances mit AWS Systems Manager finden Sie im AWS Systems Manager Benutzerhandbuch unter Systems Manager für Amazon EC2-Instances einrichten.
- Die folgende Tabelle zeigt die neuen GuardDuty verwalteten AWS Systems Manager Dokumente:

Dokumentname	Dokumenttyp	Zweck
`AmazonGuardDuty-RuntimeMonitoringSsmPlugin`	Distributor	Um den GuardDuty Security Agent zu verpacken.
`AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`	Befehl	Um das installation/un Installationsskript auszuführen, um den GuardDuty Security Agent zu installieren.

Weitere Informationen AWS Systems Manager dazu finden Sie in den Amazon EC2 Systems Manager-Dokumenten im AWS Systems Manager Benutzerhandbuch.

> **Für Debian-Server**
>
> Für die Amazon Machine Images (AMIs) für Debian Server, die von bereitgestellt werden, AWS müssen Sie den AWS Systems Manager Agenten (SSM-Agent) installieren. Sie müssen einen zusätzlichen Schritt ausführen, um den SSM-Agenten zu installieren, damit Ihre Amazon EC2 Debian Server-Instanzen SSM verwaltet werden können. Informationen zu den Schritten, die Sie ergreifen müssen, finden Sie im Benutzerhandbuch unter Manuelles Installieren des SSM-Agenten auf Debian-Server-Instances. AWS Systems Manager

Um den GuardDuty Agenten für die Amazon EC2-Instance zu installieren, verwenden Sie AWS Systems Manager

1. Öffnen Sie die AWS Systems Manager Konsole unter. https://console.aws.amazon.com/systems-manager/
2. Wählen Sie im Navigationsbereich Dokumente aus
3. Wählen Sie unter Owner by Amazon die Option aus`AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`.
4. Wählen Sie Run Command (Befehl ausführen) aus.
5. Geben Sie die folgenden Parameter für die Befehlsausführung ein
   - Aktion: Wählen Sie Installieren.
   - Installationstyp: Wählen Sie Installieren oder Deinstallieren.
   - Name: `AmazonGuardDuty-RuntimeMonitoringSsmPlugin`
   - Version: Wenn dieses Feld leer bleibt, erhalten Sie die neueste Version des GuardDuty Security Agents. Weitere Informationen zu den Release-Versionen finden Sie unterGuardDuty Security Agent-Versionen für Amazon EC2-Instances.
6. Wählen Sie die Amazon EC2-Zielinstanz aus. Sie können eine oder mehrere Amazon EC2-Instances auswählen. Weitere Informationen finden Sie im AWS Systems Manager Benutzerhandbuch unter Befehle von der Konsole AWS Systems Manager ausführen
7. Überprüfen Sie, ob die GuardDuty Agenteninstallation fehlerfrei ist. Weitere Informationen finden Sie unter Überprüfung des Installationsstatus des GuardDuty Security Agents.

Methode 2: Verwenden von Linux-Paketmanagern

Mit dieser Methode können Sie den GuardDuty Security Agent installieren, indem Sie RPM- oder Debian-Skripte ausführen. Je nach Betriebssystem können Sie eine bevorzugte Methode wählen:

- Verwenden Sie RPM-Skripte, um den Security Agent auf den Betriebssystem-Distributionen AL2, AL2023 RedHat, CentOS oder Fedora zu installieren.
- Verwenden Sie Debian-Skripte, um den Security Agent auf den Betriebssystem-Distributionen Ubuntu oder Debian zu installieren. Hinweise zu den unterstützten Ubuntu- und Debian-Betriebssystem-Distributionen finden Sie unter. Überprüfen Sie die architektonischen Anforderungen

RPM installation

> **Important**
>
> Wir empfehlen, die RPM-Signatur des GuardDuty Security Agents zu überprüfen, bevor Sie ihn auf Ihrem Computer installieren.

1. Überprüfen Sie die GuardDuty RPM-Signatur des Security Agents

   a. Bereiten Sie die Vorlage vor

   Bereiten Sie die Befehle mit dem entsprechenden öffentlichen Schlüssel, der Signatur von x86_64 RPM, der Signatur von arm64 RPM und dem entsprechenden Zugriffslink zu den in Amazon S3-Buckets gehosteten RPM-Skripten vor. Ersetzen Sie den Wert von AWS-Region, AWS Konto-ID und GuardDuty Agentenversion, um auf die RPM-Skripts zuzugreifen.

   - Öffentlicher Schlüssel:

   ```
   s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.16.0/
   publickey.pem
   ```

   - GuardDuty RPM-Signatur des Sicherheitsagenten:

Signatur von x86_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.16.0/
x86_64/amazon-guardduty-agent-1.16.0.x86_64.sig
```

Signatur von arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.16.0/arm64/
amazon-guardduty-agent-1.16.0.arm64.sig
```

- Greifen Sie auf Links zu den RPM-Skripten im Amazon S3-Bucket zu:

  Zugangslink für x86_64 RPM

  ```
  s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.16.0/
  x86_64/amazon-guardduty-agent-1.16.0.x86_64.rpm
  ```

  Zugangslink für arm64 RPM

  ```
  s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.16.0/arm64/
  amazon-guardduty-agent-1.16.0.arm64.rpm
  ```

AWS-Region	Name der Region	AWS Konto-ID
eu-west-1	Europa (Irland)	694911143906
us-east-1	USA Ost (Nord-Virginia)	593207742271
us-west-2	USA West (Oregon)	733349766148
eu-west-3	Europa (Paris)	665651866788
us-east-2	USA Ost (Ohio)	307168627858
eu-central-1	Europa (Frankfurt)	323658145986
ap-northeast-2	Asien-Pazifik (Seoul)	914738172881
eu-north-1	Europa (Stockholm)	591436053604

ap-east-1	Asien-Pazifik (Hongkong)	258348409381
me-south-1	Middle East (Bahrain)	536382113932
eu-west-2	Europa (London)	892757235363
ap-northeast-1	Asien-Pazifik (Tokio)	533107202818
ap-southeast-1	Asien-Pazifik (Singapur)	174946120834
ap-south-1	Asien-Pazifik (Mumbai)	251508486986
ap-southeast-3	Asien-Pazifik (Jakarta)	510637619217
sa-east-1	Südamerika (São Paulo)	758426053663
ap-northeast-3	Asien-Pazifik (Osaka)	273192626886
eu-south-1	Europa (Milan)	266869475730
af-south-1	Afrika (Kapstadt)	197869348890
ap-southeast-2	Asien-Pazifik (Sydney)	005257825471
me-central-1	Naher Osten (VAE)	000014521398
us-west-1	USA West (Nordkali fornien)	684579721401
ca-central-1	Kanada (Zentral)	354763396469
ca-west-1	Kanada West (Calgary)	339712888787
ap-south-2	Asien-Pazifik (Hyderabad)	950823858135
eu-south-2	Europa (Spain)	919611009337
eu-central-2	Europa (Zürich)	529164026651
ap-southeast-4	Asien-Pazifik (Melbourne)	251357961535
ap-southeast-7	Asien-Pazifik (Thailand)	054037130133

il-central-1	Israel (Tel Aviv)	870907303882
mx-central-1	Mexiko (Zentral)	982081086614
ap-east-2	Asien-Pazifik (Taipeh)	259886477082

b. Laden Sie die Vorlage herunter

Stellen Sie beim folgenden Befehl zum Herunterladen des entsprechenden öffentlichen Schlüssels, der Signatur von x86_64 RPM, der Signatur von arm64 RPM und des entsprechenden Zugriffslinks zu den in Amazon S3-Buckets gehosteten RPM-Skripten sicher, dass Sie die Konto-ID durch die entsprechende AWS-Konto ID und die Region durch Ihre aktuelle Region ersetzen.

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.16.0/
x86_64/amazon-guardduty-agent-1.16.0.x86_64.rpm ./amazon-guardduty-
agent-1.16.0.x86_64.rpm
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.16.0/
x86_64/amazon-guardduty-agent-1.16.0.x86_64.sig ./amazon-guardduty-
agent-1.16.0.x86_64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.16.0/
publickey.pem ./publickey.pem
```

c. Importieren Sie den öffentlichen Schlüssel

Verwenden Sie den folgenden Befehl, um den öffentlichen Schlüssel in die Datenbank zu importieren:

```
gpg --import publickey.pem
```

gpg zeigt den Import erfolgreich an

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
```

d. Verifiziere die Signatur

Verwenden Sie den folgenden Befehl, um die Signatur zu überprüfen

```
gpg --verify amazon-guardduty-agent-1.16.0.x86_64.sig amazon-guardduty-
agent-1.16.0.x86_64.rpm
```

Wenn die Überprüfung erfolgreich ist, wird eine Meldung angezeigt, die dem folgenden Ergebnis ähnelt. Sie können jetzt mit der Installation des GuardDuty Security Agents mithilfe von RPM fortfahren.

Beispielausgabe:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: Good signature from "AwsGuardDuty"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the
 owner.
Primary key fingerprint: 7478 91EF 5378 1334 4456  7603 06C9 06A7 093F F49D
```

Schlägt die Überprüfung fehl, bedeutet dies, dass die Signatur auf RPM möglicherweise manipuliert wurde. Sie müssen den öffentlichen Schlüssel aus der Datenbank entfernen und den Überprüfungsprozess erneut versuchen.

Beispiel:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: BAD signature from "AwsGuardDuty"
```

Verwenden Sie den folgenden Befehl, um den öffentlichen Schlüssel aus der Datenbank zu entfernen:

```
gpg --delete-keys AwsGuardDuty
```

Versuchen Sie nun erneut, den Überprüfungsprozess durchzuführen.

2. Stellen Sie eine SSH-Verbindung von Linux oder macOS aus her.
3. Installieren Sie den GuardDuty Security Agent mithilfe des folgenden Befehls:

```
sudo rpm -ivh amazon-guardduty-agent-1.16.0.x86_64.rpm
```

4. Überprüfen Sie, ob die GuardDuty Agenteninstallation fehlerfrei ist. Weitere Informationen zu den Schritten finden Sie unter[Überprüfung des Installationsstatus des GuardDuty Security Agents](#).

Debian installation

> **Important**
>
> Wir empfehlen, die Debian-Signatur des GuardDuty Security Agents zu überprüfen, bevor Sie ihn auf Ihrem Computer installieren.

1. Überprüfen Sie die GuardDuty Debian-Signatur des Security Agents

   a. Bereiten Sie Vorlagen für den entsprechenden öffentlichen Schlüssel, die Signatur des amd64-Debian-Pakets, die Signatur des arm64-Debian-Pakets und den entsprechenden Zugriffslink zu den Debian-Skripten vor, die in Amazon S3-Buckets gehostet werden

      Ersetzen Sie in den folgenden Vorlagen den Wert von, AWS Konto-ID und GuardDuty Agentenversion, um auf die Debian-Paketskripte zuzugreifen. AWS-Region

      - Öffentlicher Schlüssel:

        ```
        s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.16.0/
        publickey.pem
        ```

      - GuardDuty Debian-Signatur des Sicherheitsagenten:

        Signatur von amd64

        ```
        s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.16.0/amd64/
        amazon-guardduty-agent-1.16.0.amd64.sig
        ```

        Signatur von arm64

        ```
        s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.16.0/arm64/
        amazon-guardduty-agent-1.16.0.arm64.sig
        ```

      - Greifen Sie auf Links zu den Debian-Skripten im Amazon S3-Bucket zu:

Zugangslink für amd64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.16.0/amd64/
amazon-guardduty-agent-1.16.0.amd64.deb
```

Zugangslink für arm64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.16.0/arm64/
amazon-guardduty-agent-1.16.0.arm64.deb
```

AWS-Region	Name der Region	AWS Konto-ID
eu-west-1	Europa (Irland)	694911143906
us-east-1	USA Ost (Nord-Virginia)	593207742271
us-west-2	USA West (Oregon)	733349766148
eu-west-3	Europa (Paris)	665651866788
us-east-2	USA Ost (Ohio)	307168627858
eu-central-1	Europa (Frankfurt)	323658145986
ap-northeast-2	Asien-Pazifik (Seoul)	914738172881
eu-north-1	Europa (Stockholm)	591436053604
ap-east-1	Asien-Pazifik (Hongkong)	258348409381
me-south-1	Middle East (Bahrain)	536382113932
eu-west-2	Europa (London)	892757235363
ap-northeast-1	Asien-Pazifik (Tokio)	533107202818
ap-southeast-1	Asien-Pazifik (Singapur)	174946120834
ap-south-1	Asien-Pazifik (Mumbai)	251508486986

ap-southeast-3	Asien-Pazifik (Jakarta)	510637619217
sa-east-1	Südamerika (São Paulo)	758426053663
ap-northeast-3	Asien-Pazifik (Osaka)	273192626886
eu-south-1	Europa (Milan)	266869475730
af-south-1	Afrika (Kapstadt)	197869348890
ap-southeast-2	Asien-Pazifik (Sydney)	005257825471
me-central-1	Naher Osten (VAE)	000014521398
us-west-1	USA West (Nordkali fornien)	684579721401
ca-central-1	Kanada (Zentral)	354763396469
ca-west-1	Kanada West (Calgary)	339712888787
ap-south-2	Asien-Pazifik (Hyderabad)	950823858135
eu-south-2	Europa (Spain)	919611009337
eu-central-2	Europa (Zürich)	529164026651
ap-southeast-4	Asien-Pazifik (Melbourne)	251357961535
il-central-1	Israel (Tel Aviv)	870907303882
mx-central-1	Mexiko (Zentral)	982081086614
ap-east-2	Asien-Pazifik (Taipeh)	259886477082

b. Laden Sie den entsprechenden öffentlichen Schlüssel, die Signatur von amd64, die Signatur von arm64 und den entsprechenden Zugriffslink zu den Debian-Skripten herunter, die in Amazon S3-Buckets gehostet werden

   Ersetzen Sie in den folgenden Befehlen die Konto-ID durch die entsprechende AWS-Konto ID und die Region durch Ihre aktuelle Region.

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.16.0/
amd64/amazon-guardduty-agent-1.16.0.amd64.deb ./amazon-guardduty-
agent-1.16.0.amd64.deb
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.16.0/
amd64/amazon-guardduty-agent-1.16.0.amd64.sig ./amazon-guardduty-
agent-1.16.0.amd64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.16.0/
publickey.pem ./publickey.pem
```

c. Importieren Sie den öffentlichen Schlüssel in die Datenbank

```
gpg --import publickey.pem
```

gpg zeigt den Import erfolgreich an

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
```

d. Verifiziere die Signatur

```
gpg --verify amazon-guardduty-agent-1.16.0.amd64.sig amazon-guardduty-
agent-1.16.0.amd64.deb
```

Nach einer erfolgreichen Überprüfung wird eine Meldung angezeigt, die dem folgenden Ergebnis ähnelt:

Beispielausgabe:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: Good signature from "AwsGuardDuty"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the
 owner.
Primary key fingerprint: 7478 91EF 5378 1334 4456  7603 06C9 06A7 093F F49D
```

Sie können jetzt mit der Installation des GuardDuty Security Agents mithilfe von Debian fortfahren.

Wenn die Überprüfung jedoch fehlschlägt, bedeutet dies, dass die Signatur im Debian-Paket möglicherweise manipuliert wurde.

Beispiel:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: BAD signature from "AwsGuardDuty"
```

Verwenden Sie den folgenden Befehl, um den öffentlichen Schlüssel aus der Datenbank zu entfernen:

```
gpg --delete-keys AwsGuardDuty
```

Versuchen Sie nun erneut, den Überprüfungsprozess durchzuführen.

2. Stellen Sie eine SSH-Verbindung von Linux oder macOS aus her.
3. Installieren Sie den GuardDuty Security Agent mithilfe des folgenden Befehls:

```
sudo dpkg -i amazon-guardduty-agent-1.16.0.amd64.deb
```

4. Überprüfen Sie, ob die GuardDuty Agenteninstallation fehlerfrei ist. Weitere Informationen zu den Schritten finden Sie unterÜberprüfung des Installationsstatus des GuardDuty Security Agents.

Fehler aufgrund unzureichenden Speichers

Wenn bei der manuellen Installation oder Aktualisierung des GuardDuty Security Agents für Amazon EC2 ein `out-of-memory` Fehler auftritt, finden Sie weitere Informationen unterBehebung eines Fehlers wegen unzureichenden Speichers.

Überprüfung des Installationsstatus des GuardDuty Security Agents

Nachdem Sie die Schritte zur Installation des GuardDuty Security Agents durchgeführt haben, überprüfen Sie den Status des Agents mit den folgenden Schritten:

Um zu überprüfen, ob der GuardDuty Security Agent fehlerfrei ist

1. Stellen Sie von Linux oder macOS aus eine SSH-Verbindung her.

2. Führen Sie den folgenden Befehl aus, um den Status des GuardDuty Security Agents zu überprüfen:

```
sudo systemctl status amazon-guardduty-agent
```

Wenn Sie die Installationsprotokolle des Security Agents einsehen möchten, finden Sie sie unter/`var/log/amzn-guardduty-agent/`.

Um die Protokolle einzusehen, tun Sie dies`sudo journalctl -u amazon-guardduty-agent`.

Manuelles Aktualisieren des GuardDuty Security Agents für die Amazon EC2-Instance

GuardDuty veröffentlicht Updates für die Security Agent-Versionen. Wenn Sie den Security Agent manuell verwalten, sind Sie dafür verantwortlich, den Agenten für Ihre Amazon EC2-Instances zu aktualisieren. Informationen zu neuen Agentenversionen finden Sie unter GuardDuty Release-Versionen des Security Agents für Amazon EC2-Instances. Informationen zum Erhalt von Benachrichtigungen über eine neue Version der Agentenversion finden Sie unterAmazon GuardDuty SNS SNS-Ankündigungen abonnieren.

Um den Security Agent für die Amazon EC2-Instance manuell zu aktualisieren

Der Vorgang zum Aktualisieren des Security Agents ist identisch mit der Installation des Security Agents. Je nachdem, mit welcher Methode Sie den Agenten installiert haben, können Sie die Schritte Manuelles Installieren des Security Agents für Amazon EC2-Instances ausführen.

Wenn Sie Methode 1 — Durch verwenden verwenden AWS Systems Manager, können Sie den Security Agent mithilfe des Befehls Run aktualisieren. Verwenden Sie die Agent-Version, auf die Sie aktualisieren möchten.

Wenn Sie Methode 2 — Mithilfe von Linux-Paketmanagern verwenden, können Sie die im Manuelles Installieren des Security Agents Abschnitt angegebenen Skripts verwenden. Die Skripts enthalten bereits die neueste Agenten-Release-Version. Informationen zu kürzlich veröffentlichten Agentenversionen finden Sie unterGuardDuty Security Agent-Versionen für Amazon EC2-Instances.

Nach dem Update des Security Agents können Sie den Installationsstatus anhand der Protokolle überprüfen. Weitere Informationen finden Sie unter Überprüfung des Installationsstatus des GuardDuty Security Agents.

Verwaltung des GuardDuty Sicherheitsagenten auf Bottlerocket (Amazon ECS auf Amazon EC2)

Important

Diese Seite bezieht sich nur auf ECS-optimized Bottlerocket-AMIS-Versionen `v1.62.1` und höher, einschließlich der folgenden Varianten:

- `bottlerocket-aws-ecs-2-x86_64` / `bottlerocket-aws-ecs-2-aarch64`
- `bottlerocket-aws-ecs-3-x86_64` / `bottlerocket-aws-ecs-3-aarch64`
- `bottlerocket-aws-ecs-2-nvidia` / `bottlerocket-aws-ecs-2-nvidia-fips`
- `bottlerocket-aws-ecs-3-nvidia` / `bottlerocket-aws-ecs-3-nvidia-fips`

Für Bottlerocket-Instances in Amazon EKS-Clustern verwendet Runtime Monitoring ein anderes Setup. Siehe Voraussetzungen für die Unterstützung von Amazon EKS-Clustern.

Auf dieser Seite wird erklärt, wie der GuardDuty Security Agent auf ECS-optimized Bottlerocket-AMIs läuft und wie er bereitgestellt wird. GuardDuty Auf Bottlerocket läuft der Agent als Host-Container und nicht als installiertes RPM- oder Debian-Paket. Bottlerocket ist ein containeroptimiertes Linux-Betriebssystem mit einem unveränderlichen Root-Dateisystem, daher werden keine herkömmlichen Paketmanager verwendet. GuardDuty hostet das Agent-Container-Image in einem Amazon Elastic Container Registry (Amazon ECR) -Repository, das es verwaltet. Wenn Sie Runtime Monitoring mit automatisierter Agentenkonfiguration aktivieren, GuardDuty verwendet AWS Systems Manager Distributor, um den Agent-Host-Container für Sie bereitzustellen.

Voraussetzungen

Bevor Sie fortfahren, stellen Sie sicher, dass Sie alle Anweisungen befolgen. Voraussetzungen für die ECS-EC2 Bottlerocket-Unterstützung

Automatische Agentenkonfiguration aktivieren

ECS-EC2 Bottlerocket-Instances verwenden dasselbe SSM-Dokument und dieselbe automatisierte Agentenkonfiguration wie standardmäßige Amazon EC2-Instances. Um den GuardDuty automatisierten Agenten für Ihre Bottlerocket-Instances zu aktivieren, folgen Sie den Schritten unter. Automatisierter Agent auf der Amazon EC2-Ressource Dies umfasst:

- Aktivierung des GuardDuty Agenten in einer Umgebung mit mehreren Konten.
- Aktivierung des GuardDuty automatisierten Agenten in einem eigenständigen Konto.

Weitere Voraussetzungen für die Verwendung von Inklusions- oder Ausschluss-Tags finden Sie unterBei Verwendung der automatisierten Agentenkonfiguration.

Der Agent wird verifiziert

Nachdem Sie die automatische Agentenkonfiguration aktiviert haben, stellen Sie sicher, dass der Agent auf Ihrer Bottlerocket-Instance ausgeführt wird:

1. Stellen Sie mithilfe des SSM Session Manager eine Verbindung zu Ihrer Instanz her.
2. Geben Sie den Admin-Container ein:`enter-admin-container`.
3. Überprüfen Sie die Agentenprotokolle mithilfe einer der folgenden Optionen:
   - `sheltie journalctl -u host-containers@amazon-guardduty-agent`
   - Aus einer Sheltie-Sitzung (`sudo sheltie`):`ls /var/log/amzn-guardduty-agent/`.

Informationen zur Überprüfung der Abdeckungsstatistiken für Ihre Amazon EC2-Instances finden Sie unter. Überprüfen der Abdeckungsstatistiken

Wenn der Abdeckungsstatus als Ungesund angezeigt wird, finden Sie unter. Behebung von Problemen mit der Bottlerocket-Runtime-Abdeckung ECS-EC2

Verwaltung des automatisierten Sicherheitsagenten für Fargate (nur Amazon ECS)

Runtime Monitoring unterstützt die Verwaltung des Sicherheitsagenten für Ihre Amazon ECS-Cluster (AWS Fargate) nur über GuardDuty. Die manuelle Verwaltung des Security Agents auf Amazon ECS-Clustern wird nicht unterstützt.

Bevor Sie mit den Schritten in diesem Abschnitt fortfahren, stellen Sie sicher, dass Sie die folgenden Schritte ausführenVoraussetzungen für AWS Fargate Unterstützung (nur Amazon ECS).

Wählen Sie auf der Grundlage von eine bevorzugte Methode ausAnsätze zur Verwaltung von GuardDuty Sicherheitsagenten in ECS-Fargate Amazon-Ressourcen, um den GuardDuty automatisierten Agenten für Ihre Ressourcen zu aktivieren.

Konfiguration des GuardDuty Agenten für eine Umgebung mit mehreren Konten

In einer Umgebung mit mehreren Konten kann nur das delegierte GuardDuty Administratorkonto die automatische Agentenkonfiguration für die Mitgliedskonten aktivieren oder deaktivieren und die automatische Agentenkonfiguration für Amazon ECS-Cluster verwalten, die zu den Mitgliedskonten in ihrer Organisation gehören. Ein GuardDuty Mitgliedskonto kann diese Konfiguration nicht ändern. Das delegierte GuardDuty Administratorkonto verwaltet seine Mitgliedskonten mithilfe von AWS Organizations. Weitere Informationen zu Umgebungen mit mehreren Konten finden Sie unter Verwalten mehrerer Konten in. GuardDuty

Aktivierung der automatisierten Agentenkonfiguration für ein delegiertes Administratorkonto GuardDuty

Manage for all Amazon ECS clusters (account level)

Wenn Sie für Runtime Monitoring die Option Für alle Konten aktivieren ausgewählt haben, haben Sie die folgenden Optionen:

- Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Für alle Konten aktivieren. GuardDuty wird den Security Agent für alle Amazon ECS-Aufgaben bereitstellen und verwalten, die gestartet werden.
- Wählen Sie Konten manuell konfigurieren.

Wenn Sie im Abschnitt Runtime Monitoring die Option Konten manuell konfigurieren ausgewählt haben, gehen Sie wie folgt vor:

1. Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Konten manuell konfigurieren aus.
2. Wählen Sie im Abschnitt Konto für delegierte GuardDuty Administratoren (dieses Konto) die Option Aktivieren aus.

Wählen Sie Speichern.

Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Dienstes sind, ist nach der Aktivierung der Laufzeitüberwachung eine neue Dienstbereitstellung erforderlich. Wenn die letzte Bereitstellung für einen bestimmten ECS-Dienst gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst mithilfe von Folgendes aktualisieren`forceNewDeployment`.

Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

- Aktualisieren eines Amazon ECS-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
- UpdateServicein der Amazon Elastic Container Service API-Referenz.
- update-service in der AWS CLI Befehlsreferenz.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Fügen Sie diesem Amazon ECS-Cluster ein Tag mit dem Schlüssel-Wert-Paar als - hinzu. `GuardDutyManaged` `false`
2. Verhindern Sie die Änderung von Tags, außer durch vertrauenswürdige Entitäten. Die unter Verhindern, dass Tags nur aufgrund autorisierter Prinzipien im AWS Organizations Benutzerhandbuch geändert werden, wurde so geändert, dass sie auch hier gilt.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
```

```
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
```

```
            }
        }
    ]
}
```

3. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
4. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
5.

> **Note**
>
> Fügen Sie Ihren Amazon ECS-Clustern immer das Ausschluss-Tag hinzu, bevor Sie die automatische Agentenkonfiguration für Ihr Konto aktivieren. Andernfalls wird der GuardDuty Sidecar-Container an alle Container in den Amazon ECS-Aufgaben angehängt, die gestartet werden.

   Wählen Sie auf der Registerkarte „Konfiguration“ in der automatisierten Agentenkonfiguration die Option „Aktivieren“ aus.

   Für die Amazon ECS-Cluster, die nicht ausgeschlossen wurden, GuardDuty wird die Bereitstellung des Security Agents im Sidecar-Container verwaltet.
6. Wählen Sie Speichern.
7. Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Service sind, ist eine neue Servicebereitstellung erforderlich, nachdem Sie Runtime Monitoring aktiviert haben. Wenn die letzte Bereitstellung für einen bestimmten ECS-Dienst gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst mithilfe von Folgendes aktualisieren`forceNewDeployment`.

   Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

   - Aktualisieren eines Amazon ECS-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
   - UpdateServicein der Amazon Elastic Container Service API-Referenz.
   - update-service in der AWS CLI Befehlsreferenz.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Fügen Sie einem Amazon ECS-Cluster, für den Sie alle Aufgaben einschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar muss - sein. `GuardDutyManaged` `true`
2. Verhindern Sie die Änderung dieser Tags, außer durch vertrauenswürdige Entitäten. Die Richtlinie unter Verhindern, dass Tags nur aufgrund autorisierter Prinzipien im AWS Organizations Benutzerhandbuch geändert werden, wurde dahingehend geändert, dass sie auch hier gilt.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
```

```
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Wenn Sie Inklusion-Tags für Ihre Amazon ECS-Cluster verwenden, müssen Sie den GuardDuty Agenten nicht explizit über die automatische Agentenkonfiguration aktivieren.

3. Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Service sind, ist nach der Aktivierung von Runtime Monitoring eine neue Servicebereitstellung erforderlich. Wenn die letzte Bereitstellung für einen bestimmten ECS-Dienst gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst mithilfe von Folgendes aktualisieren`forceNewDeployment`.

   Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

   - Aktualisieren eines Amazon ECS-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
   - UpdateServicein der Amazon Elastic Container Service API-Referenz.
   - update-service in der AWS CLI Befehlsreferenz.

Auto-enable für alle Mitgliedskonten

Manage for all Amazon ECS clusters (account level)

Bei den folgenden Schritten wird davon ausgegangen, dass Sie im Abschnitt Runtime Monitoring die Option Für alle Konten aktivieren ausgewählt haben.

1. Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Für alle Konten aktivieren aus. GuardDuty wird den Security Agent für alle Amazon ECS-Aufgaben bereitstellen und verwalten, die gestartet werden.
2. Wählen Sie Speichern.
3. Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Service sind, ist eine neue Servicebereitstellung erforderlich, nachdem Sie Runtime Monitoring aktiviert haben. Wenn die letzte Bereitstellung für einen bestimmten ECS-Dienst gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst mithilfe von Folgendes aktualisieren`forceNewDeployment`.

Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

- Aktualisieren eines Amazon ECS-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
- UpdateServicein der Amazon Elastic Container Service API-Referenz.
- update-service in der AWS CLI Befehlsreferenz.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Fügen Sie diesem Amazon ECS-Cluster ein Tag mit dem Schlüssel-Wert-Paar als - hinzu. `GuardDutyManaged` `false`
2. Verhindern Sie die Änderung von Tags, außer durch vertrauenswürdige Entitäten. Die unter Verhindern, dass Tags nur aufgrund autorisierter Prinzipien im AWS Organizations Benutzerhandbuch geändert werden, wurde so geändert, dass sie auch hier gilt.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
```

```
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
```

```
                }
            }
        }
    ]
}
```

3. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
4. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
5.

> **Note**
>
> Fügen Sie Ihren Amazon ECS-Clustern immer das Ausschluss-Tag hinzu, bevor Sie die automatische Agentenkonfiguration für Ihr Konto aktivieren. Andernfalls wird der GuardDuty Sidecar-Container an alle Container in den Amazon ECS-Aufgaben angehängt, die gestartet werden.

   Wählen Sie auf der Registerkarte Konfiguration die Option Bearbeiten aus.
6. Wählen Sie im Abschnitt Automatische Agentenkonfiguration die Option Für alle Konten aktivieren

   Für die Amazon ECS-Cluster, die nicht ausgeschlossen wurden, GuardDuty wird die Bereitstellung des Sicherheitsagenten im Sidecar-Container verwaltet.
7. Wählen Sie Speichern.
8. Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Service sind, ist eine neue Servicebereitstellung erforderlich, nachdem Sie Runtime Monitoring aktiviert haben. Wenn die letzte Bereitstellung für einen bestimmten ECS-Dienst gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst mithilfe von Folgendes aktualisieren`forceNewDeployment`.

   Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

   - Aktualisieren eines Amazon ECS-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
   - UpdateServicein der Amazon Elastic Container Service API-Referenz.
   - update-service in der AWS CLI Befehlsreferenz.

Manage for selective (inclusion-only) Amazon ECS clusters (cluster level)

Unabhängig davon, wie Sie Runtime Monitoring aktivieren, helfen Ihnen die folgenden Schritte dabei, ausgewählte Amazon ECS Fargate-Aufgaben für alle Mitgliedskonten in Ihrer Organisation zu überwachen.

1. Aktivieren Sie keine Konfiguration im Abschnitt Automatisierte Agentenkonfiguration. Behalten Sie die Runtime Monitoring-Konfiguration bei, die Sie im vorherigen Schritt ausgewählt haben.
2. Wählen Sie Speichern.
3. Verhindern Sie die Änderung dieser Tags, außer durch vertrauenswürdige Entitäten. Die Richtlinie unter Verhindern, dass Tags nur aufgrund autorisierter Prinzipien im AWS Organizations Benutzerhandbuch geändert werden, wurde dahingehend geändert, dass sie auch hier gilt.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
```

```
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
```

```
        }
    ]
}
```

> **Note**
>
> Wenn Sie Inklusion-Tags für Ihre Amazon ECS-Cluster verwenden, müssen Sie die automatische GuardDuty Agentenverwaltung nicht explizit aktivieren.

4. Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Service sind, ist eine neue Servicebereitstellung erforderlich, nachdem Sie Runtime Monitoring aktiviert haben. Wenn die letzte Bereitstellung für einen bestimmten ECS-Dienst gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst mithilfe von Folgendes aktualisieren`forceNewDeployment`.

   Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

   - Aktualisieren eines Amazon ECS-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
   - UpdateServicein der Amazon Elastic Container Service API-Referenz.
   - update-service in der AWS CLI Befehlsreferenz.

Aktivierung der automatisierten Agentenkonfiguration für bestehende aktive Mitgliedskonten

Manage for all Amazon ECS clusters (account level)

1. Auf der Seite Runtime Monitoring können Sie auf der Registerkarte Konfiguration den aktuellen Status der automatisierten Agentenkonfiguration einsehen.
2. Wählen Sie im Bereich für die automatische Agentenkonfiguration im Abschnitt Aktive Mitgliedskonten die Option Aktionen aus.
3. Wählen Sie bei Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten.
4. Wählen Sie Bestätigen aus.
5. Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Dienstes sind, ist nach der Aktivierung der Laufzeitüberwachung eine neue Dienstbereitstellung erforderlich. Wenn die letzte Bereitstellung für einen bestimmten ECS-Dienst gestartet wurde, bevor Sie Runtime

Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst mithilfe von Folgendes aktualisieren`forceNewDeployment`.

Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

- Aktualisieren eines Amazon ECS-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
- UpdateServicein der Amazon Elastic Container Service API-Referenz.
- update-service in der AWS CLI Befehlsreferenz.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Fügen Sie diesem Amazon ECS-Cluster ein Tag mit dem Schlüssel-Wert-Paar als - hinzu. `GuardDutyManaged` `false`
2. Verhindern Sie die Änderung von Tags, außer durch vertrauenswürdige Entitäten. Die unter Verhindern, dass Tags nur aufgrund autorisierter Prinzipien im AWS Organizations Benutzerhandbuch geändert werden, wurde so geändert, dass sie auch hier gilt.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
```

```
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
```

```
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
4. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
5.

> **Note**
>
> Fügen Sie Ihren Amazon ECS-Clustern immer das Ausschluss-Tag hinzu, bevor Sie die automatische Agentenkonfiguration für Ihr Konto aktivieren. Andernfalls wird der GuardDuty Sidecar-Container an alle Container in den Amazon ECS-Aufgaben angehängt, die gestartet werden.

   Wählen Sie auf der Registerkarte „Konfiguration“ im Abschnitt „Automatisierte Agentenkonfiguration“ unter „Aktive Mitgliedskonten“ die Option „Aktionen“ aus.
6. Wählen Sie bei Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten.

   Für die Amazon ECS-Cluster, die nicht ausgeschlossen wurden, GuardDuty wird die Bereitstellung des Sicherheitsagenten im Sidecar-Container verwaltet.
7. Wählen Sie Bestätigen aus.
8. Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Service sind, ist eine neue Servicebereitstellung erforderlich, nachdem Sie Runtime Monitoring aktiviert haben. Wenn die letzte Bereitstellung für einen bestimmten ECS-Dienst gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst mithilfe von Folgendes aktualisieren`forceNewDeployment`.

   Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

   - Aktualisieren eines Amazon ECS-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
   - UpdateServicein der Amazon Elastic Container Service API-Referenz.
   - update-service in der AWS CLI Befehlsreferenz.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Fügen Sie einem Amazon ECS-Cluster, für den Sie alle Aufgaben einschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar muss - sein. `GuardDutyManaged` `true`
2. Verhindern Sie die Änderung dieser Tags, außer durch vertrauenswürdige Entitäten. Die Richtlinie unter Verhindern, dass Tags nur aufgrund autorisierter Prinzipien im AWS Organizations Benutzerhandbuch geändert werden, wurde dahingehend geändert, dass sie auch hier gilt.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
```

```
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Wenn Sie Inklusion-Tags für Ihre Amazon ECS-Cluster verwenden, müssen Sie die automatische Agentenkonfiguration nicht explizit aktivieren.

3. Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Service sind, ist eine neue Servicebereitstellung erforderlich, nachdem Sie Runtime Monitoring aktiviert haben. Wenn die letzte Bereitstellung für einen bestimmten ECS-Dienst gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst mithilfe von Folgendes aktualisieren`forceNewDeployment`.

   Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

   - Aktualisieren eines Amazon ECS-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
   - UpdateServicein der Amazon Elastic Container Service API-Referenz.
   - update-service in der AWS CLI Befehlsreferenz.

Auto-enable Automatisierte Agentenkonfiguration für neue Mitglieder

Manage for all Amazon ECS clusters (account level)

1. Wählen Sie auf der Seite Runtime Monitoring die Option Bearbeiten aus, um die bestehende Konfiguration zu aktualisieren.
2. Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Automatisch für neue Mitgliedskonten aktivieren aus.
3. Wählen Sie Speichern.
4. Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Dienstes sind, ist eine neue Dienstbereitstellung erforderlich, nachdem Sie Runtime Monitoring aktiviert haben. Wenn die letzte Bereitstellung für einen bestimmten ECS-Dienst gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst mithilfe von Folgendes aktualisieren`forceNewDeployment`.

   Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

- Aktualisieren eines Amazon ECS-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
- UpdateServicein der Amazon Elastic Container Service API-Referenz.
- update-service in der AWS CLI Befehlsreferenz.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Fügen Sie diesem Amazon ECS-Cluster ein Tag mit dem Schlüssel-Wert-Paar als - hinzu. `GuardDutyManaged` `false`
2. Verhindern Sie die Änderung von Tags, außer durch vertrauenswürdige Entitäten. Die Richtlinie unter Verhindern, dass Tags nur aufgrund autorisierter Prinzipien im AWS Organizations Benutzerhandbuch geändert werden, wurde so geändert, dass sie auch hier gilt.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
```

```
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
```

```
            }
        }
    ]
}
```

3. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
4. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
5.

> **Note**
>
> Fügen Sie Ihren Amazon ECS-Clustern immer das Ausschluss-Tag hinzu, bevor Sie die automatische Agentenkonfiguration für Ihr Konto aktivieren. Andernfalls wird der GuardDuty Sidecar-Container an alle Container in den Amazon ECS-Aufgaben angehängt, die gestartet werden.

   Wählen Sie auf der Registerkarte Konfiguration im Abschnitt Automatisierte Agentenkonfiguration die Option Automatisch für neue Mitgliedskonten aktivieren aus.

   Für die Amazon ECS-Cluster, die nicht ausgeschlossen wurden, GuardDuty wird die Bereitstellung des Sicherheitsagenten im Sidecar-Container verwaltet.
6. Wählen Sie Speichern.
7. Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Service sind, ist eine neue Servicebereitstellung erforderlich, nachdem Sie Runtime Monitoring aktiviert haben. Wenn die letzte Bereitstellung für einen bestimmten ECS-Dienst gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst mithilfe von Folgendes aktualisieren`forceNewDeployment`.

   Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

   - Aktualisieren eines Amazon ECS-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
   - UpdateServicein der Amazon Elastic Container Service API-Referenz.
   - update-service in der AWS CLI Befehlsreferenz.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Fügen Sie einem Amazon ECS-Cluster, für den Sie alle Aufgaben einschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar muss - sein. `GuardDutyManaged` `true`
2. Verhindern Sie die Änderung dieser Tags, außer durch vertrauenswürdige Entitäten. Die Richtlinie unter Verhindern, dass Tags nur aufgrund autorisierter Prinzipien im AWS Organizations Benutzerhandbuch geändert werden, wurde dahingehend geändert, dass sie auch hier gilt.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
```

```
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Wenn Sie Inklusion-Tags für Ihre Amazon ECS-Cluster verwenden, müssen Sie die automatische Agentenkonfiguration nicht explizit aktivieren.

3. Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Service sind, ist eine neue Servicebereitstellung erforderlich, nachdem Sie Runtime Monitoring aktiviert haben. Wenn die letzte Bereitstellung für einen bestimmten ECS-Dienst gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst mithilfe von Folgendes aktualisieren`forceNewDeployment`.

   Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

   - Aktualisieren eines Amazon ECS-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
   - UpdateServicein der Amazon Elastic Container Service API-Referenz.
   - update-service in der AWS CLI Befehlsreferenz.

Selektives Aktivieren der automatisierten Agentenkonfiguration für aktive Mitgliedskonten

Manage for all Amazon ECS (account level)

1. Wählen Sie auf der Seite Konten die Konten aus, für die Sie die Monitoring-Automated Runtime-Agent-Konfiguration aktivieren möchten (ECS-Fargate). Sie können mehrere Konten auswählen. Stellen Sie sicher, dass die Konten, die Sie in diesem Schritt auswählen, bereits für Runtime Monitoring aktiviert sind.
2. Wählen Sie unter Schutzpläne bearbeiten die entsprechende Option aus, um die Runtime Monitoring-Automated Agent-Konfiguration zu aktivieren (ECS-Fargate).
3. Wählen Sie Bestätigen aus.
4. Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Dienstes sind, ist eine neue Dienstbereitstellung erforderlich, nachdem Sie Runtime Monitoring aktiviert haben. Wenn die letzte Bereitstellung für einen bestimmten ECS-Dienst gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst mithilfe von Folgendes aktualisieren`forceNewDeployment`.

   Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

- Aktualisieren eines Amazon ECS-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
- UpdateServicein der Amazon Elastic Container Service API-Referenz.
- update-service in der AWS CLI Befehlsreferenz.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Fügen Sie diesem Amazon ECS-Cluster ein Tag mit dem Schlüssel-Wert-Paar als - hinzu. `GuardDutyManaged` `false`
2. Verhindern Sie die Änderung von Tags, außer durch vertrauenswürdige Entitäten. Die Richtlinie unter Verhindern, dass Tags nur aufgrund autorisierter Prinzipien im AWS Organizations Benutzerhandbuch geändert werden, wurde so geändert, dass sie auch hier gilt.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
```

```
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
```

```
            }
        }
    ]
}
```

3. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
4. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
5.

> **Note**
>
> Fügen Sie Ihren Amazon ECS-Clustern immer das Ausschluss-Tag hinzu, bevor Sie die automatische GuardDuty Agentenverwaltung für Ihr Konto aktivieren. Andernfalls wird der GuardDuty Sidecar-Container an alle Container in den Amazon ECS-Aufgaben angehängt, die gestartet werden.

   Wählen Sie auf der Seite Konten die Konten aus, für die Sie die Monitoring-Automated Runtime-Agent-Konfiguration aktivieren möchten (). ECS-Fargate Sie können mehrere Konten auswählen. Stellen Sie sicher, dass die Konten, die Sie in diesem Schritt auswählen, bereits für Runtime Monitoring aktiviert sind.

   Für die Amazon ECS-Cluster, die nicht ausgeschlossen wurden, GuardDuty wird die Bereitstellung des Sicherheitsagenten im Sidecar-Container verwaltet.
6. Wählen Sie unter Schutzpläne bearbeiten die entsprechende Option aus, um die Monitoring-Automated Runtime-Agent-Konfiguration zu aktivieren ()ECS-Fargate.
7. Wählen Sie Speichern.
8. Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Dienstes sind, ist eine neue Dienstbereitstellung erforderlich, nachdem Sie Runtime Monitoring aktiviert haben. Wenn die letzte Bereitstellung für einen bestimmten ECS-Dienst gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst mithilfe von Folgendes aktualisieren`forceNewDeployment`.

   Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

   - Aktualisieren eines Amazon ECS-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
   - UpdateServicein der Amazon Elastic Container Service API-Referenz.
   - update-service in der AWS CLI Befehlsreferenz.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Stellen Sie sicher, dass Sie die automatische Agentenkonfiguration (oder die Monitoring-Automated Runtime-Agent-Konfiguration (ECS-Fargate)) nicht für die ausgewählten Konten aktivieren, die über die Amazon ECS-Cluster verfügen, die Sie überwachen möchten.
2. Fügen Sie einem Amazon ECS-Cluster, für den Sie alle Aufgaben einschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar muss - sein. `GuardDutyManaged` `true`
3. Verhindern Sie die Änderung dieser Tags, außer durch vertrauenswürdige Entitäten. Die Richtlinie unter Verhindern, dass Tags nur aufgrund autorisierter Prinzipien im AWS Organizations Benutzerhandbuch geändert werden, wurde dahingehend geändert, dass sie auch hier gilt.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
```

```
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
```

```
}
```

> **Note**
>
> Wenn Sie Inklusion-Tags für Ihre Amazon ECS-Cluster verwenden, müssen Sie die automatische Agentenkonfiguration nicht explizit aktivieren.

4. Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Service sind, ist eine neue Servicebereitstellung erforderlich, nachdem Sie Runtime Monitoring aktiviert haben. Wenn die letzte Bereitstellung für einen bestimmten ECS-Dienst gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst mithilfe von Folgendes aktualisieren`forceNewDeployment`.

   Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

   - Aktualisieren eines Amazon ECS-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
   - UpdateServicein der Amazon Elastic Container Service API-Referenz.
   - update-service in der AWS CLI Befehlsreferenz.

GuardDuty Agent für ein eigenständiges Konto konfigurieren

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
3. Auf der Registerkarte „Konfiguration“:

   a. Zur Verwaltung der automatisierten Agentenkonfiguration für alle Amazon ECS-Cluster (Kontoebene)

      Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration für AWS Fargate (nur ECS) die Option Aktivieren aus. Wenn eine neue Fargate-Aufgabe von Amazon ECS gestartet GuardDuty wird, wird die Bereitstellung des Sicherheitsagenten verwaltet.

      - Wählen Sie Speichern.

b. Zur Verwaltung der automatisierten Agentenkonfiguration durch Ausschluss einiger Amazon ECS-Cluster (Cluster-Ebene)

   i. Fügen Sie dem Amazon ECS-Cluster, für den Sie alle Aufgaben ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar muss - sein. `GuardDutyManaged` `false`

   ii. Verhindern Sie die Änderung dieser Tags, außer durch vertrauenswürdige Entitäten. Die Richtlinie unter Verhindern, dass Tags nur aufgrund autorisierter Prinzipien im AWS Organizations Benutzerhandbuch geändert werden, wurde dahingehend geändert, dass sie auch hier gilt.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn":
 "arn:aws:iam::123456789012:role/org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
```

```
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn":
 "arn:aws:iam::123456789012:role/org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn":
 "arn:aws:iam::123456789012:role/org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

iii. Wählen Sie auf der Registerkarte „Konfiguration“ im Abschnitt „Automatisierte Agentenkonfiguration“ die Option „Aktivieren“.

> **Note**
>
> Fügen Sie Ihrem Amazon ECS-Cluster immer das Ausschluss-Tag hinzu, bevor Sie die automatische GuardDuty Agentenverwaltung für Ihr Konto aktivieren. Andernfalls wird der Security Agent für alle Aufgaben eingesetzt, die innerhalb des entsprechenden Amazon ECS-Clusters gestartet werden.

Für die Amazon ECS-Cluster, die nicht ausgeschlossen wurden, GuardDuty wird die Bereitstellung des Security Agents im Sidecar-Container verwaltet.

iv. Wählen Sie Speichern.

c. Zur Verwaltung der automatisierten Agentenkonfiguration durch Einbeziehung einiger Amazon ECS-Cluster (Cluster-Ebene)

i. Fügen Sie einem Amazon ECS-Cluster, für den Sie alle Aufgaben einschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar muss - sein. `GuardDutyManaged` `true`

ii. Verhindern Sie die Änderung dieser Tags, außer durch vertrauenswürdige Entitäten. Die Richtlinie unter Verhindern, dass Tags nur aufgrund autorisierter Prinzipien im AWS Organizations Benutzerhandbuch geändert werden, wurde dahingehend geändert, dass sie auch hier gilt.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
```

```
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn":
"arn:aws:iam::123456789012:role/org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn":
"arn:aws:iam::123456789012:role/org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
```

```
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn":
 "arn:aws:iam::123456789012:role/org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

4. Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Dienstes sind, ist nach der Aktivierung der Laufzeitüberwachung eine neue Dienstbereitstellung erforderlich. Wenn die letzte Bereitstellung für einen bestimmten ECS-Dienst gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst mithilfe von Folgendes aktualisieren`forceNewDeployment`.

   Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

   - Aktualisieren eines Amazon ECS-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
   - UpdateServicein der Amazon Elastic Container Service API-Referenz.
   - update-service in der AWS CLI Befehlsreferenz.

Automatische Verwaltung des Security Agents für Amazon EKS-Ressourcen

Runtime Monitoring unterstützt die Aktivierung des Security Agents durch GuardDuty automatische Konfiguration und manuell. In diesem Abschnitt werden die Schritte zur Aktivierung der automatisierten Agentenkonfiguration für Amazon EKS-Cluster beschrieben.

Bevor Sie fortfahren, stellen Sie sicher, dass Sie die befolgt habenVoraussetzungen für die Unterstützung von Amazon EKS-Clustern.

Wählen Sie die Schritte in den folgenden Abschnitten entsprechend Ihrer bevorzugten Vorgehensweise aus. Verwalten Sie den Security Agent über GuardDuty

Konfiguration des automatisierten Agenten für Umgebungen mit mehreren Konten

In Umgebungen mit mehreren Konten kann nur das delegierte GuardDuty Administratorkonto die automatische Agentenkonfiguration für die Mitgliedskonten aktivieren oder deaktivieren und den automatisierten Agenten für die EKS-Cluster verwalten, die zu den Mitgliedskonten in ihrer Organisation gehören. Die GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Das Konto des delegierten GuardDuty Administratorkontos verwaltet ihre Mitgliedskonten mithilfe von AWS Organizations. Weitere Informationen zu Umgebungen mit mehreren Konten finden Sie unter Verwaltung mehrerer Konten.

Konfiguration der automatisierten Agentenkonfiguration für das delegierte Administratorkonto GuardDuty

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Verwalten Sie den Security Agent über GuardDuty (Alle EKS-Cluster überwachen)	Wenn Sie im Abschnitt Runtime Monitoring die Option Für alle Konten aktivieren ausgewählt haben, haben Sie folgende Optionen: • Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Für alle Konten aktivieren aus. GuardDuty installiert und verwaltet den Security Agent für alle EKS-Cluster, die zum Konto des delegierten GuardDuty Administratorkontos gehören, sowie für alle EKS-Cluster, die zu allen vorhandenen und potenziell neuen Mitgliedskonten in der Organisation gehören. • Wählen Sie Konten manuell konfigurieren. Wenn Sie im Abschnitt Runtime Monitoring die Option Konten manuell konfigurieren ausgewählt haben, gehen Sie wie folgt vor: 1. Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Konten manuell konfigurieren aus.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	2. Wählen Sie im Abschnitt Konto für delegierte GuardDuty Administratoren (dieses Konto) die Option Aktivieren aus. Wählen Sie Speichern.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Alle EKS-Cluster überwachen, jedoch einige davon ausschließen (mithilfe des Ausschluss-Tags)	Wählen Sie aus den folgenden Verfahren eines der Szenarien aus, das auf Sie zutrifft. Um einen EKS-Cluster von der Überwachung auszuschließen, wenn der GuardDuty Security Agent nicht auf diesem Cluster installiert wurde 1. Fügen Sie diesem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `false` hinzu. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *`ec2:CreateTags`* durch `eks:TagResource` . • Ersetzen Sie *`ec2:DeleteTags`* durch `eks:UntagResource` . • Ersetzen Sie *`access-project`* durch `GuardDutyManaged` • *`123456789012`* Ersetzen Sie durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen:

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte

```
"aws:PrincipalArn":["arn:aws:iam::12345678901
2:role/org-admins/iam-admin", "arn:aws:iam::1234
56789012:role/org-admins/iam-admin", "arn:aws:
iam::123456789012:role/org-admins/iam-admin"]
```

3. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
4. Wählen Sie im Navigationsbereich Runtime Monitoring aus.

> **Note**
>
> Fügen Sie Ihren EKS-Clustern immer das Ausschluss-Tag hinzu, bevor Sie die automatische GuardDuty Agentenverwaltung für Ihr Konto aktivieren. Andernfalls wird der GuardDuty Security Agent auf allen EKS-Clustern in Ihrem Konto bereitgestellt.

5. Wählen Sie auf der Registerkarte Konfiguration im Abschnitt GuardDuty Agentenverwaltung die Option Aktivieren aus.

   Für die EKS-Cluster, die nicht von der Überwachung ausgeschlossen wurden, GuardDuty wird die Bereitstellung und Aktualisierung des GuardDuty Security Agents verwaltet.
6. Wählen Sie Speichern.

Um einen EKS-Cluster von der Überwachung auszuschließen, wenn der GuardDuty Security Agent auf diesem Cluster bereitgestellt wurde

1. Fügen Sie diesem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `false` hinzu.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2:CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2:DeleteTags* durch `eks:UntagResource` . • Ersetzen Sie *access-project* durch `GuardDutyManaged` • *123456789012* Ersetzen Sie durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Wenn Sie den automatisierten Agenten für diesen EKS-Cluster aktiviert hatten, GuardDuty wird der Security Agent für diesen Cluster nach diesem Schritt nicht aktualisiert. Der Security Agent bleibt jedoch weiterhin im Einsatz und empfängt GuardDuty

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	weiterhin die Runtime-Ereignisse von diesem EKS-Cluster. Dies kann sich auf Ihre Nutzungsstatistiken auswirken. Um die Laufzeit-Ereignisse von diesem Cluster nicht mehr zu empfangen, müssen Sie den bereitgestellten Sicherheitsagent aus diesem EKS-Cluster entfernen. Weitere Informationen zum Entfernen des bereitgestellten Sicherheitsagenten finden Sie unter Deaktivieren, Deinstallieren und Bereinigen von Ressourcen in Runtime Monitoring 4. Wenn Sie den GuardDuty Security Agent für diesen EKS-Cluster manuell verwaltet haben, finden Sie weitere Informationen unterDeaktivieren, Deinstallieren und Bereinigen von Ressourcen in Runtime Monitoring.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Ausgewählte EKS-Cluster mithilfe von Einschließen-Tags überwachen	Unabhängig davon, wie Sie die Laufzeitüberwachung aktivieren, helfen Ihnen die folgenden Schritte bei der Überwachung ausgewählter EKS-Cluster in Ihrem Konto: 1. Stellen Sie sicher, dass Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Deaktivieren für ein delegiertes GuardDuty Administratorkonto (dieses Konto) auswählen. Behalten Sie die Runtime Monitoring-Konfiguration so bei, wie sie im vorherigen Schritt konfiguriert wurde. 2. Wählen Sie Speichern. 3. Fügen Sie Ihrem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `true` hinzu. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für die ausgewählten EKS-Cluster, die Sie überwachen möchten. 4. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *`ec2:CreateTags`* durch `eks:TagResource` . • Ersetzen Sie *`ec2:DeleteTags`* durch `eks:UntagResource` . • Ersetzen *`access-project`* durch `GuardDutyManaged`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	• *123456789012* Ersetzen Sie durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Den GuardDuty Security Agent manuell verwalten	Unabhängig davon, wie Sie Runtime Monitoring aktivieren, können Sie den Security Agent für Ihre EKS-Cluster manuell verwalten. 1. Stellen Sie sicher, dass Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Deaktivieren für ein delegiertes GuardDuty Administratorkonto (dieses Konto) auswählen. Behalten Sie die Runtime Monitoring-Konfiguration so bei, wie sie im vorherigen Schritt konfiguriert wurde. 2. Wählen Sie Speichern. 3. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Sicherheitsagenten für den Amazon EKS-Cluster.

Auto-enable Automatisierter Agent für alle Mitgliedskonten

> **Note**
>
> Die Aktualisierung der Konfiguration der Mitgliedskonten kann bis zu 24 Stunden dauern.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Sicherheitsagenten	Schritte
Verwalten Sie den Security Agent über GuardDuty (Alle EKS-Cluster überwachen)	In diesem Thema wird die Laufzeitüberwachung für alle Mitglieds konten aktiviert. Daher wird bei den folgenden Schritten davon ausgegangen, dass Sie im Abschnitt Runtime Monitoring die Option Für alle Konten aktivieren ausgewählt haben müssen. 1. Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Für alle Konten aktivieren aus. GuardDuty installiert und verwaltet den Security Agent für alle EKS-Cluster, die zum Konto des delegierten GuardDuty Administratorkontos gehören, sowie für alle EKS-Cluster, die zu allen vorhandenen und potenziell neuen Mitgliedskonten in der Organisation gehören. 2. Wählen Sie Speichern.
Alle EKS-Cluster überwachen, jedoch einige davon ausschließen (mithilfe des Ausschluss-Tags)	Wählen Sie aus den folgenden Verfahren eines der Szenarien aus, das auf Sie zutrifft. Um einen EKS-Cluster von der Überwachung auszuschließen, wenn der GuardDuty Security Agent nicht auf diesem Cluster bereitgestellt wurde 1. Fügen Sie diesem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `false` hinzu. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte

Bevorzugter Ansatz zur Verwaltung des GuardDuty Sicherheitsagenten	Schritte

Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben:

- Ersetzen Sie *ec2:CreateTags* durch `eks:TagResource` .
- Ersetzen Sie *ec2:DeleteTags* durch `eks:UntagResource` .
- Ersetzen Sie *access-project* durch `GuardDutyManaged`
- *123456789012* Ersetzen Sie durch die AWS-Konto ID der vertrauenswürdigen Entität.

  Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen:

```
"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]
```

3. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
4. Wählen Sie im Navigationsbereich Runtime Monitoring aus.

> **Note**
>
> Fügen Sie Ihren EKS-Clustern immer das Ausschluss-Tag hinzu, bevor Sie Automated Agent für Ihr Konto aktivieren. Andernfalls wird der GuardDuty Security Agent auf allen EKS-Clustern in Ihrem Konto bereitgestellt.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Sicherheitsagenten	Schritte
	5. Wählen Sie auf der Registerkarte Konfiguration im Konfigurationsabschnitt für Runtime Monitoring die Option Bearbeiten aus. 6. Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Für alle Konten aktivieren aus. Für die EKS-Cluster, die nicht von der Überwachung ausgeschlossen wurden, GuardDuty wird die Bereitstellung und Aktualisierung des GuardDuty Security Agents verwaltet. 7. Wählen Sie Speichern. Um einen EKS-Cluster von der Überwachung auszuschließen, wenn der GuardDuty Security Agent auf diesem Cluster bereitgestellt wurde 1. Fügen Sie diesem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `false` hinzu. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch. 2. Wenn Sie die automatische Agentenkonfiguration für diesen EKS-Cluster aktiviert hatten, GuardDuty wird der Security Agent für diesen Cluster nach diesem Schritt nicht aktualisiert. Der Security Agent bleibt jedoch weiterhin im Einsatz und empfängt GuardDuty weiterhin die Runtime-Ereignisse von diesem EKS-Cluster. Dies kann sich auf Ihre Nutzungsstatistiken auswirken. Um die Laufzeit-Ereignisse von diesem Cluster nicht mehr zu empfangen, müssen Sie den bereitgestellten Sicherheitsagent aus diesem EKS-Cluster entfernen. Weitere Informationen zum Entfernen des bereitgestellten Sicherheitsagenten finden Sie

Bevorzugter Ansatz zur Verwaltung des GuardDuty Sicherheitsagenten	Schritte
	unter Deaktivieren, Deinstallieren und Bereinigen von Ressourcen in Runtime Monitoring 3. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2:CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2:DeleteTags* durch `eks:UntagResource` . • Ersetzen *access-project* durch `GuardDutyManaged` • *123456789012* Ersetzen Sie durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 4. Wenn Sie den GuardDuty Security Agent für diesen EKS-Cluster manuell verwaltet haben, finden Sie weitere Informationen unterDeaktivieren, Deinstallieren und Bereinigen von Ressourcen in Runtime Monitoring.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Sicherheitsagenten	Schritte
Ausgewählte EKS-Cluster mithilfe von Einschließen-Tags überwachen	Unabhängig davon, wie Sie die Laufzeitüberwachung aktivieren, helfen Ihnen die folgenden Schritte bei der Überwachung ausgewählter EKS-Cluster für alle Mitgliedskonten in Ihrer Organisation: 1. Aktivieren Sie keine Konfiguration im Abschnitt Automatisierte Agentenkonfiguration. Behalten Sie die Runtime Monitoring-Konfiguration so bei, wie sie im vorherigen Schritt konfiguriert wurde. 2. Wählen Sie Speichern. 3. Fügen Sie Ihrem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `true` hinzu. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für die ausgewählten EKS-Cluster, die Sie überwachen möchten. 4. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2:CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2:DeleteTags* durch `eks:UntagResource` . • Ersetzen *access-project* durch `GuardDutyManaged`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Sicherheitsagenten	Schritte
	• *123456789012* Ersetzen Sie durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Den GuardDuty Security Agent manuell verwalten	Unabhängig davon, wie Sie Runtime Monitoring aktivieren, können Sie den Security Agent für Ihre EKS-Cluster manuell verwalten. 1. Aktivieren Sie keine Konfiguration im Abschnitt Automatisierte Agentenkonfiguration. Behalten Sie die Runtime Monitoring-Konfiguration so bei, wie sie im vorherigen Schritt konfiguriert wurde. 2. Wählen Sie Speichern. 3. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Sicherheitsagenten für den Amazon EKS-Cluster.

Aktivierung des automatisierten Agenten für alle vorhandenen aktiven Mitgliedskonten

> **Note**
>
> Die Aktualisierung der Konfiguration der Mitgliedskonten kann bis zu 24 Stunden dauern.

Um den GuardDuty Security Agent für bestehende aktive Mitgliedskonten in Ihrer Organisation zu verwalten

- GuardDuty Um die Laufzeitereignisse von den EKS-Clustern zu empfangen, die zu den vorhandenen aktiven Mitgliedskonten in der Organisation gehören, müssen Sie einen bevorzugten Ansatz für die Verwaltung des GuardDuty Security Agents für diese EKS-Cluster wählen. Weitere Informationen zu diesen Ansätzen finden Sie unter Ansätze zur Verwaltung von GuardDuty Sicherheitsagenten in Amazon EKS-Clustern.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Verwalten Sie den Security Agent über GuardDuty (Alle EKS-Cluster überwachen)	So überwachen Sie alle EKS-Cluster auf allen vorhanden en aktiven Mitgliedskonten 1. Auf der Seite Runtime Monitoring können Sie auf der Registerkarte Konfiguration den aktuellen Status der automatisierten Agent-Konfiguration einsehen. 2. Wählen Sie im Bereich für die automatische Agentenkonfiguration im Abschnitt Aktive Mitglieds konten die Option Aktionen aus. 3. Wählen Sie bei Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten. 4. Wählen Sie Bestätigen aus.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Alle EKS-Cluster überwachen, jedoch einige davon ausschließen (mithilfe des Ausschluss-Tags)	Wählen Sie aus den folgenden Verfahren eines der Szenarien aus, das auf Sie zutrifft. Um einen EKS-Cluster von der Überwachung auszuschließen, wenn der GuardDuty Security Agent nicht auf diesem Cluster bereitgestellt wurde 1. Fügen Sie diesem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `false` hinzu. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *`ec2:CreateTags`* durch `eks:TagResource` . • Ersetzen Sie *`ec2:DeleteTags`* durch `eks:UntagResource` . • Ersetzen Sie *`access-project`* durch `GuardDutyManaged` • *`123456789012`* Ersetzen Sie durch die AWS-Konto ID der vertrauenswürdigen Entität.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/. 4. Wählen Sie im Navigationsbereich Runtime Monitoring aus. **Note** Fügen Sie Ihren EKS-Clustern immer das Ausschluss-Tag hinzu, bevor Sie die automatische Agentenkonfiguration für Ihr Konto aktivieren. Andernfalls wird der GuardDuty Security Agent auf allen EKS-Clustern in Ihrem Konto bereitgestellt. 5. Wählen Sie auf der Registerkarte Konfiguration im Bereich Automatisierte Agentenkonfiguration unter Aktive Mitgliedskonten die Option Aktionen aus. 6. Wählen Sie bei Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten. 7. Wählen Sie Bestätigen aus.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Um einen EKS-Cluster von der Überwachung auszuschl ießen, nachdem der GuardDuty Security Agent bereits auf diesem Cluster installiert wurde 1. Fügen Sie diesem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `false` hinzu. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutze rhandbuch. Nach diesem Schritt GuardDuty wird der Security Agent für diesen Cluster nicht aktualisiert. Der Security Agent bleibt jedoch weiterhin im Einsatz und empfängt GuardDuty weiterhin die Runtime-E reignisse von diesem EKS-Cluster. Dies kann sich auf Ihre Nutzungsstatistiken auswirken. 2. Um zu verhindern, dass Tags, außer durch vertrauen swürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *`ec2:CreateTags`* durch `eks:TagResource` . • Ersetzen Sie *`ec2:DeleteTags`* durch `eks:UntagResource` .

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	• Ersetzen *access-project* durch `GuardDuty Managed` • *123456789012* Ersetzen Sie durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Unabhängig davon, wie Sie den Security Agent verwalten (durch GuardDuty oder manuell), müssen Sie den bereitgestellten Security Agent aus diesem EKS-Cluster entfernen, um den Empfang der Laufzeitereignisse von diesem Cluster zu beenden. Weitere Informationen zum Entfernen des bereitgestellten Sicherheitsagenten finden Sie unter Deaktivieren, Deinstallieren und Bereinigen von Ressourcen in Runtime Monitoring.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Ausgewählte EKS-Cluster mithilfe von Einschließen-Tags überwachen	1. Nachdem Sie Runtime Monitoring aktiviert haben, aktivieren Sie auf der Seite Konten nicht die Option Runtime Monitoring — Automatisierte Agentenkonfiguration. 2. Fügen Sie dem EKS-Cluster ein Tag hinzu, das zu dem ausgewählten Konto gehört, das Sie überwachen möchten. Das Schlüssel-Wert-Paar des Tags muss `GuardDutyManaged -true` sein. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für die ausgewählten EKS-Cluster, die Sie überwachen möchten. 3. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *`ec2:CreateTags`* durch `eks:TagResource` . • Ersetzen Sie *`ec2:DeleteTags`* durch `eks:UntagResource` . • Ersetzen *`access-project`* durch `GuardDuty Managed`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	• *123456789012* Ersetzen Sie durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Den GuardDuty Security Agent manuell verwalten	1. Stellen Sie sicher, dass Sie im Abschnitt Automatisierte Agentenkonfiguration nicht die Option Aktivieren auswählen. Halten Sie Runtime Monitoring aktiviert. 2. Wählen Sie Speichern. 3. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Sicherheitsagenten für den Amazon EKS-Cluster.

Auto-enable automatische Agentenkonfiguration für neue Mitglieder

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Verwalten Sie den Security Agent über GuardDuty (Alle EKS-Cluster überwachen)	1. Wählen Sie auf der Seite Runtime Monitoring die Option Bearbeiten aus, um die bestehende Konfiguration zu aktualisieren.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	2. Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Automatisch für neue Mitgliedskonten aktivieren aus. 3. Wählen Sie Speichern.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Alle EKS-Cluster überwachen, jedoch einige davon ausschließen (mithilfe des Ausschluss-Tags)	Wählen Sie aus den folgenden Verfahren eines der Szenarien aus, das auf Sie zutrifft. Um einen EKS-Cluster von der Überwachung auszuschließen, wenn der GuardDuty Security Agent nicht auf diesem Cluster bereitgestellt wurde 1. Fügen Sie diesem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `false` hinzu. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *`ec2:CreateTags`* durch `eks:TagResource` . • Ersetzen Sie *`ec2:DeleteTags`* durch `eks:UntagResource` . • Ersetzen Sie *`access-project`* durch `GuardDutyManaged` • *`123456789012`* Ersetzen Sie durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen:

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	<pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 3. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/. 4. Wählen Sie im Navigationsbereich Runtime Monitoring aus. **Note** Fügen Sie Ihren EKS-Clustern immer das Ausschluss-Tag hinzu, bevor Sie die automatische Agentenkonfiguration für Ihr Konto aktivieren. Andernfalls wird der GuardDuty Security Agent auf allen EKS-Clustern in Ihrem Konto bereitgestellt. 5. Wählen Sie auf der Registerkarte Konfiguration im Bereich GuardDuty Agentenverwaltung die Option Automatisch für neue Mitgliedskonten aktivieren aus. Für die EKS-Cluster, die nicht von der Überwachung ausgeschlossen wurden, GuardDuty wird die Bereitstellung und Aktualisierung des GuardDuty Security Agents verwaltet. 6. Wählen Sie Speichern.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Um einen EKS-Cluster von der Überwachung auszuschließen, wenn der GuardDuty Security Agent auf diesem Cluster bereitgestellt wurde 1. Unabhängig davon, ob Sie den GuardDuty Security Agent über GuardDuty oder manuell verwalten, fügen Sie diesem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als hinzu`false`. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch. Wenn Sie den Automated Agent für diesen EKS-Cluster aktiviert hatten, GuardDuty wird der Security Agent für diesen Cluster nach diesem Schritt nicht aktualisiert. Der Security Agent bleibt jedoch weiterhin im Einsatz und empfängt GuardDuty weiterhin die Runtime-Ereignisse von diesem EKS-Cluster. Dies kann sich auf Ihre Nutzungsstatistiken auswirken. Um die Laufzeit-Ereignisse von diesem Cluster nicht mehr zu empfangen, müssen Sie den bereitgestellten Sicherheitsagent aus diesem EKS-Cluster entfernen. Weitere Informationen zum Entfernen des bereitgestellten Sicherheitsagenten finden Sie unter Deaktivieren, Deinstallieren und Bereinigen von Ressourcen in Runtime Monitoring 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben:

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	• Ersetzen Sie *ec2:CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2:DeleteTags* durch `eks:UntagResource` . • Ersetzen *access-project* durch `GuardDuty Managed` • *123456789012* Ersetzen Sie durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Wenn Sie den GuardDuty Security Agent für diesen EKS-Cluster manuell verwaltet haben, finden Sie weitere Informationen unterDeaktivieren, Deinstallieren und Bereinigen von Ressourcen in Runtime Monitoring.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Ausgewählte EKS-Cluster mithilfe von Einschließen-Tags überwachen	Unabhängig davon, wie Sie die Laufzeitüberwachung aktiviert haben, helfen Ihnen die folgenden Schritte dabei, ausgewählte EKS-Cluster für die neuen Mitgliedskonten in Ihrer Organisation zu überwachen. 1. Stellen Sie sicher, dass im Abschnitt Automatisierte Agentenkonfiguration die Option Automatisch für neue Mitgliedskonten aktivieren deaktiviert ist. Behalten Sie die Runtime Monitoring-Konfiguration so bei, wie sie im vorherigen Schritt konfiguriert wurde. 2. Wählen Sie Speichern. 3. Fügen Sie Ihrem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `true` hinzu. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für die ausgewählten EKS-Cluster, die Sie überwachen möchten. 4. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *`ec2:CreateTags`* durch `eks:TagResource`. • Ersetzen Sie *`ec2:DeleteTags`* durch `eks:UntagResource`.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	• Ersetzen *access-project* durch `GuardDuty Managed` • *123456789012* Ersetzen Sie durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Verwalten Sie den GuardDuty Security Agent manuell	Unabhängig davon, wie Sie Runtime Monitoring aktivieren, können Sie den Security Agent für Ihre EKS-Cluster manuell verwalten. 1. Stellen Sie sicher, dass im Abschnitt Automatische Agentenkonfiguration das Kontrollkästchen Automatisch für neue Mitgliedskonten aktivieren deaktiviert ist. Behalten Sie die Runtime Monitoring-Konfiguration so bei, wie sie im vorherigen Schritt konfiguriert wurde. 2. Wählen Sie Speichern. 3. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Sicherheitsagenten für den Amazon EKS-Cluster.

Selektive Konfiguration des automatisierten Agenten für aktive Mitgliedskonten

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Verwalten Sie den Security Agent über GuardDuty (Alle EKS-Cluster überwachen)	1. Wählen Sie auf der Seite Konten die Konten aus, für die Sie die automatische Agentenkonfiguration aktivieren möchten. Sie können mehr als ein Konto zur gleichen Zeit auswählen. Stellen Sie sicher, dass für die Konten, die Sie in diesem Schritt auswählen, EKS-Laufzeit-Überwachung bereits aktiviert ist. 2. Wählen Sie unter Schutzpläne bearbeiten die entsprechende Option aus, um Runtime Monitoring — Automatisierte Agentenkonfiguration zu aktivieren. 3. Wählen Sie Bestätigen aus.
Alle EKS-Cluster überwachen, jedoch einige davon ausschließen (mithilfe des Ausschluss-Tags)	Wählen Sie aus den folgenden Verfahren eines der Szenarien aus, das auf Sie zutrifft. Um einen EKS-Cluster von der Überwachung auszuschließen, wenn der GuardDuty Security Agent nicht auf diesem Cluster bereitgestellt wurde 1. Fügen Sie diesem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `false` hinzu. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben:

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	• Ersetzen Sie *ec2:CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2:DeleteTags* durch `eks:UntagResource` . • Ersetzen Sie *access-project* durch `GuardDuty Managed` • *123456789012* Ersetzen Sie durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/. **Note** Fügen Sie Ihren EKS-Clustern immer das Ausschluss-Tag hinzu, bevor Sie die automatische Agent-Konfiguration für Ihr Konto aktivieren. Andernfalls wird der GuardDuty Security Agent auf allen EKS-Clustern in Ihrem Konto bereitgestellt. 4. Wählen Sie auf der Kontenseite das Konto aus, für das Sie Agent automatisch verwalten aktivieren möchten. Sie können mehr als ein Konto zur gleichen Zeit auswählen.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	5. Wählen Sie unter Schutzpläne bearbeiten die entsprechende Option aus, um die Monitoring-Automated Runtime-Agent-Konfiguration für das ausgewählte Konto zu aktivieren. Für die EKS-Cluster, die nicht von der Überwachung ausgeschlossen wurden, GuardDuty wird die Bereitstellung und Aktualisierung des GuardDuty Security Agents verwaltet. 6. Wählen Sie Speichern. Um einen EKS-Cluster von der Überwachung auszuschließen, wenn der GuardDuty Security Agent auf diesem Cluster bereitgestellt wurde 1. Fügen Sie diesem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `false` hinzu. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch. Wenn Sie zuvor die automatische Agentenkonfiguration für diesen EKS-Cluster aktiviert hatten, GuardDuty wird der Security Agent für diesen Cluster nach diesem Schritt nicht aktualisiert. Der Security Agent bleibt jedoch weiterhin im Einsatz und empfängt GuardDuty weiterhin die Runtime-Ereignisse von diesem EKS-Cluster. Dies kann sich auf Ihre Nutzungsstatistiken auswirken. Um die Laufzeit-Ereignisse von diesem Cluster nicht mehr zu empfangen, müssen Sie den bereitgestellten Sicherheitsagent aus diesem EKS-Cluster entfernen. Weitere Informationen zum Entfernen des bereitgestellten Sicherheitsagenten finden Sie

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	unter Deaktivieren, Deinstallieren und Bereinigen von Ressourcen in Runtime Monitoring 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2:CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2:DeleteTags* durch `eks:UntagResource` . • Ersetzen *access-project* durch `GuardDutyManaged` • *123456789012* Ersetzen Sie durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Wenn Sie den GuardDuty Security Agent für diesen EKS-Cluster manuell verwaltet haben, müssen Sie ihn entfernen. Weitere Informationen finden Sie unter Deaktivieren, Deinstallieren und Bereinigen von Ressourcen in Runtime Monitoring.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Ausgewählte EKS-Cluster mithilfe von Einschließen-Tags überwachen	Unabhängig davon, wie Sie die Laufzeitüberwachung aktivieren, helfen Ihnen die folgenden Schritte bei der Überwachung ausgewählter EKS-Cluster, die zu den ausgewählten Konten gehören: 1. Stellen Sie sicher, dass Sie die Runtime Monitoring-Automated Agent-Konfiguration nicht für die ausgewählten Konten aktivieren, die über die EKS-Cluster verfügen, die Sie überwachen möchten. 2. Fügen Sie Ihrem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `true` hinzu. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch. Nach dem Hinzufügen des Tags verwaltet GuardDuty es die Bereitstellung und Aktualisierung des Security Agents für die ausgewählten EKS-Cluster, die Sie überwachen möchten. 3. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *`ec2:CreateTags`* durch `eks:TagResource` . • Ersetzen Sie *`ec2:DeleteTags`* durch `eks:UntagResource` . • Ersetzen *`access-project`* durch `GuardDutyManaged` • *`123456789012`* Ersetzen Sie durch die AWS-Konto ID der vertrauenswürdigen Entität.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Verwalten Sie den GuardDuty Security Agent manuell	1. Behalten Sie die Runtime Monitoring-Konfiguration so bei, wie sie im vorherigen Schritt konfiguriert wurde. Stellen Sie sicher, dass Sie Runtime Monitoring — Automatisierte Agentenkonfiguration für keines der ausgewählten Konten aktivieren. 2. Wählen Sie Bestätigen aus. 3. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Sicherheitsagenten für den Amazon EKS-Cluster.

Konfiguration des automatisierten Agenten für ein eigenständiges Konto

Ein eigenständiges Konto besitzt die Entscheidung, ob ein Schutzpaket AWS-Konto in einem bestimmten Bereich aktiviert oder deaktiviert werden soll AWS-Region.

Wenn Ihr Konto durch oder durch AWS Organizations die Einladungsmethode mit einem GuardDuty Administratorkonto verknüpft ist, gilt dieser Abschnitt nicht für Ihr Konto. Weitere Informationen finden Sie unter Aktivierung von Runtime Monitoring für Umgebungen mit mehreren Konten.

Nachdem Sie Runtime Monitoring aktiviert haben, stellen Sie sicher, dass der GuardDuty Security Agent durch automatische Konfiguration oder manuelle Bereitstellung installiert wird. Stellen Sie sicher, dass Sie den Security Agent installieren, um alle im folgenden Verfahren aufgeführten Schritte abzuschließen.

Wählen Sie je nach Ihrer Präferenz, alle oder ausgewählte Amazon EKS-Ressourcen zu überwachen, eine bevorzugte Methode aus und folgen Sie den Schritten in der folgenden Tabelle.

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
3. Wählen Sie auf der Registerkarte Konfiguration die Option Aktivieren aus, um die automatische Agentenkonfiguration für Ihr Konto zu aktivieren.

Bevorzugter Ansatz für die Bereitstellung des GuardDuty Security Agents	Schritte
Verwalten Sie den Security Agent über GuardDuty (Alle EKS-Cluster überwachen)	1. Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Aktivieren aus. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle vorhandenen und potenziell neuen EKS-Cluster in Ihrem Konto. 2. Wählen Sie Speichern.
Alle EKS-Cluster überwachen, jedoch einige davon ausschließen (mithilfe des Ausschluss-Tags)	Wählen Sie aus den folgenden Verfahren eines der Szenarien aus, das auf Sie zutrifft. Um einen EKS-Cluster von der Überwachung auszuschließen, wenn der GuardDuty Security Agent nicht auf diesem Cluster bereitgestellt wurde 1. Fügen Sie diesem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `false` hinzu. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden

Bevorzugter Ansatz für die Bereitstellung des GuardDuty Security Agents	Schritte
	Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2:CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2:DeleteTags* durch `eks:UntagResource` . • Ersetzen Sie *access-project* durch `GuardDutyManaged` • *123456789012* Ersetzen Sie durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/. 4. Wählen Sie im Navigationsbereich Runtime Monitoring aus.

Bevorzugter Ansatz für die Bereitstellung des GuardDuty Security Agents	Schritte
	Note Fügen Sie Ihren EKS-Clustern immer das Ausschluss-Tag hinzu, bevor Sie die automatische GuardDuty Agentenverwaltung für Ihr Konto aktivieren. Andernfalls wird der GuardDuty Security Agent auf allen EKS-Clustern in Ihrem Konto bereitgestellt. 5. Wählen Sie auf der Registerkarte „Konfiguration“ im Abschnitt „GuardDuty Agentenverwaltung“ die Option „Aktivieren“ aus. Für die EKS-Cluster, die nicht von der Überwachung ausgeschlossen wurden, GuardDuty wird die Bereitstellung und Aktualisierung des GuardDuty Security Agents verwaltet. 6. Wählen Sie Speichern. Um einen EKS-Cluster von der Überwachung auszuschließen, nachdem der GuardDuty Security Agent bereits auf diesem Cluster bereitgestellt wurde 1. Fügen Sie diesem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `false` hinzu. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch.

Bevorzugter Ansatz für die Bereitstellung des GuardDuty Security Agents	Schritte
	Nach diesem Schritt GuardDuty wird der Security Agent für diesen Cluster nicht aktualisiert. Der Security Agent bleibt jedoch weiterhin im Einsatz und empfängt GuardDuty weiterhin die Runtime-E reignisse von diesem EKS-Cluster. Dies kann sich auf Ihre Nutzungsstatistiken auswirken. 2. Um zu verhindern, dass Tags, außer durch vertrauen swürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2:CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2:DeleteTags* durch `eks:UntagResource` . • Ersetzen *access-project* durch `GuardDuty Managed` • *123456789012* Ersetzen Sie durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:`

Bevorzugter Ansatz für die Bereitstellung des GuardDuty Security Agents	Schritte

	<pre>iam::123456789012:role/org-admins/ia
	m-admin"]</pre>
	3. Um die Laufzeit-Ereignisse von diesem Cluster nicht mehr zu empfangen, müssen Sie den bereitgestellten Sicherheitsagent aus diesem EKS-Cluster entfernen. Weitere Informationen zum Entfernen des bereitgestellten Sicherheitsagenten finden Sie unter Deaktivieren, Deinstallieren und Bereinigen von Ressourcen in Runtime Monitoring.

Bevorzugter Ansatz für die Bereitstellung des GuardDuty Security Agents	Schritte
Ausgewählte EKS-Cluster mithilfe von Einschließen-Tags überwachen	1. Stellen Sie sicher, dass Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Deaktivieren auswählen. Lassen Sie die Laufzeitüberwachung aktiviert. 2. Wählen Sie Speichern. 3. Fügen Sie diesem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `true` hinzu. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für die ausgewählten EKS-Cluster, die Sie überwachen möchten. 4. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *`ec2:CreateTags`* durch `eks:TagResource`. • Ersetzen Sie *`ec2:DeleteTags`* durch `eks:UntagResource`. • Ersetzen *`access-project`* durch `GuardDutyManaged`

Bevorzugter Ansatz für die Bereitstellung des GuardDuty Security Agents	Schritte
	• *123456789012* Ersetzen Sie durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Den Agent manuell verwalten	1. Stellen Sie sicher, dass Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Deaktivieren auswählen. Lassen Sie die Laufzeitüberwachung aktiviert. 2. Wählen Sie Speichern. 3. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Sicherheitsagenten für den Amazon EKS-Cluster.

Manuelles Verwalten des Sicherheitsagenten für den Amazon EKS-Cluster

In diesem Abschnitt wird beschrieben, wie Sie Ihren Amazon EKS-Zusatzagenten (GuardDuty Agenten) verwalten können, nachdem Sie Runtime Monitoring (oder EKS Runtime Monitoring) aktiviert haben. Um Runtime Monitoring verwenden zu können, müssen Sie Runtime Monitoring aktivieren und das Amazon EKS-Add-on konfigurieren`aws-guardduty-agent`. Sie müssen beide Schritte ausführen, um potenzielle Bedrohungen GuardDuty zu erkennen und zu generierenGuardDuty Findetypen für die Laufzeitüberwachung.

Für die manuelle Verwaltung des Agenten müssen Sie als Voraussetzung einen VPC-Endpunkt erstellen. Dies hilft beim GuardDuty Empfangen der Laufzeitereignisse. Danach können Sie den Security Agent installieren, sodass er GuardDuty die Laufzeitereignisse von den Amazon EKS-Ressourcen empfängt. Wenn eine neue Agentenversion für diese Ressource GuardDuty veröffentlicht wird, können Sie die Agentenversion in Ihrem Konto aktualisieren.

Themen

- Voraussetzung — Erstellen eines Amazon VPC-Endpunkts
- Manuelles Installieren des GuardDuty Security Agents auf Amazon EKS-Ressourcen
- Manuelles Aktualisieren des Security Agents für Amazon EKS-Ressourcen

Voraussetzung — Erstellen eines Amazon VPC-Endpunkts

Bevor Sie den GuardDuty Security Agent installieren können, müssen Sie einen Amazon Virtual Private Cloud (Amazon VPC) -Endpunkt erstellen. Dies hilft dabei, die Laufzeitereignisse Ihrer Amazon EKS-Ressourcen zu GuardDuty empfangen.

> **Note**
>
> Für die Nutzung des VPC-Endpunkts fallen keine zusätzlichen Kosten an.

Wählen Sie eine bevorzugte Zugriffsmethode, um einen Amazon VPC-Endpunkt zu erstellen.

Console

Um einen VPC-Endpunkt zu erstellen

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsmenü unter Virtual Private Cloud die Option Endpunkte.
3. Klicken Sie auf Endpunkt erstellen.
4. Wählen Sie auf der Seite Endpunkt erstellen für Servicekategorie die Option Andere Endpunkt-Services.
5. Geben Sie unter Servicename **`com.amazonaws.`*`us-east-1`*`.guardduty-data`** ein.

   Stellen Sie sicher, dass Sie es *`us-east-1`* durch die richtige Region ersetzen. Dies muss dieselbe Region wie der EKS-Cluster sein, der zu Ihrer AWS-Konto ID gehört.

6. Wählen Sie Service verifizieren.
7. Nachdem der Servicename erfolgreich verifiziert wurde, wählen Sie die VPC aus, in der sich Ihr Cluster befindet. Fügen Sie die folgende Richtlinie hinzu, um die Nutzung von VPC-Endpunkten auf das angegebene Konto zu beschränken. Unter Angabe der unter dieser Richtlinie angegebenen Organisations-`Condition` können Sie die folgende Richtlinie aktualisieren, um den Zugriff auf Ihren Endpunkt einzuschränken. Informationen zur Bereitstellung von VPC-Endpunktunterstützung für bestimmte Konto-IDs in Ihrer Organisation finden Sie unter Organization condition to restrict access to your endpoint.

   JSON

```
{
 "Version":"2012-10-17",
 "Statement": [
  {
   "Action": "*",
   "Resource": "*",
   "Effect": "Allow",
   "Principal": "*"
  },
  {
   "Condition": {
    "StringNotEquals": {
     "aws:PrincipalAccount": "111122223333"
    }
   },
   "Action": "*",
   "Resource": "*",
   "Effect": "Deny",
   "Principal": "*"
  }
 ]
}
```

   Die `aws:PrincipalAccount`-Konto-ID muss mit dem Konto übereinstimmen, das die VPC und den VPC-Endpunkt enthält. Die folgende Liste zeigt, wie Sie den VPC-Endpunkt mit anderen AWS-Konto -IDs teilen können:

Organisationsbedingung , um den Zugriff auf Ihren Endpunkt einzuschränken

- Um mehrere Konten für den Zugriff auf den VPC-Endpunkt anzugeben, ersetzen Sie `"aws:PrincipalAccount": "111122223333"` durch Folgendes:

```
"aws:PrincipalAccount": [
          "666666666666",
          "555555555555"
    ]
```

- Um allen Mitgliedern einer Organisation den Zugriff auf den VPC-Endpunkt zu ermöglichen, ersetzen Sie `"aws:PrincipalAccount": "111122223333"` durch Folgendes:

```
"aws:PrincipalOrgID": "o-abcdef0123"
```

- Um den Zugriff auf eine Ressource auf eine Organisations-ID zu beschränken, fügen Sie Ihre `ResourceOrgID` zur Richtlinie hinzu.

  Weitere Informationen finden Sie unter ResourceOrg ID.

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. Wählen Sie unter Zusätzliche Einstellungen die Option DNS-Name aktivieren.
9. Wählen Sie unter Subnetze die Subnetze aus, in denen sich Ihr Cluster befindet.
10. Wählen Sie unter Sicherheitsgruppen eine Sicherheitsgruppe aus, für die der eingehende Port 443 von Ihrer VPC (oder Ihrem EKS-Cluster) aktiviert ist. Wenn Sie noch keine Sicherheitsgruppe haben, für die der eingehende Port 443 aktiviert ist, Erstellen Sie eine Sicherheitsgruppe.

    Wenn beim Einschränken der eingehenden Berechtigungen für Ihre VPC (oder Instance) ein Problem auftritt, können Sie den eingehenden 443-Port von einer beliebigen IP-Adresse aus verwenden. `(0.0.0.0/0)` Es wird jedoch GuardDuty empfohlen, IP-Adressen zu verwenden, die dem CIDR-Block für Ihre VPC entsprechen. Weitere Informationen finden Sie unter VPC-CIDR-Blöcke im Amazon VPC-Benutzerhandbuch.

API/CLI

Um einen VPC-Endpunkt zu erstellen

- Aufrufen CreateVpcEndpoint.
- Verwenden Sie die folgenden Werte für die Parameter:
  - Geben Sie unter Servicename **`com.amazonaws.`*`us-east-1`*`.guardduty-data`** ein.

    Stellen Sie sicher, dass Sie es *`us-east-1`* durch die richtige Region ersetzen. Dies muss dieselbe Region sein wie der EKS-Cluster, der zu Ihrer AWS-Konto ID gehört.
  - Aktivieren Sie für DNSOptions die private DNS-Option, indem Sie sie auf `true` setzen.
- Weitere Informationen finden Sie AWS Command Line Interface unter create-vpc-endpoint.

Nachdem Sie die Schritte befolgt haben, finden Sie unter Validierung der VPC-Endpunktkonfiguration Um sicherzustellen, dass der VPC-Endpunkt korrekt eingerichtet wurde.

Manuelles Installieren des GuardDuty Security Agents auf Amazon EKS-Ressourcen

In diesem Abschnitt wird beschrieben, wie Sie den GuardDuty Security Agent zum ersten Mal für bestimmte EKS-Cluster bereitstellen können. Bevor Sie mit diesem Abschnitt fortfahren, stellen Sie sicher, dass Sie die Voraussetzungen bereits eingerichtet und Runtime Monitoring für Ihre Konten aktiviert haben. Der GuardDuty Security Agent (EKS-Add-on) funktioniert nicht, wenn Sie Runtime Monitoring nicht aktivieren.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um den GuardDuty Security Agent zum ersten Mal einzusetzen.

Console

1. Öffnen Sie die Amazon EKS-Konsole unter https://console.aws.amazon.com/eks/home #/clusters.
2. Wählen Sie Ihren Clusternamen aus.
3. Wählen Sie die Registerkarte Add-ons aus.
4. Wählen Sie Weitere Add-Ons erhalten.
5. Wählen Sie auf der Seite „Add-Ons auswählen“ die Option Amazon GuardDuty EKS Runtime Monitoring aus.
6. GuardDuty empfiehlt, die neueste und standardmäßige Agentenversion auszuwählen.

7. Verwenden Sie auf der Seite Ausgewählte Add-On-Einstellungen konfigurieren die Standardeinstellungen. Wenn der Status Ihres EKS-Add-ons Aktivierung erfordert lautet, wählen Sie Aktivieren GuardDuty. Diese Aktion öffnet die GuardDuty Konsole, um Runtime Monitoring für Ihre Konten zu konfigurieren.
8. Nachdem Sie Runtime Monitoring für Ihre Konten konfiguriert haben, wechseln Sie zurück zur Amazon EKS-Konsole. Der Status Ihres EKS-Add-Ons sollte sich auf Bereit zur Installation geändert haben.
9. (Optional) Bereitstellung des EKS-Add-On-Konfigurationsschemas

   Wenn Sie für die Zusatzversion v1.5.0 oder höher wählen, unterstützt Runtime Monitoring die Konfiguration bestimmter Parameter des GuardDuty Agenten. Hinweise zu Parameterbereichen finden Sie unterKonfigurieren Sie EKS-Add-On-Parameter.

   a. Erweitern Sie Optionale Konfigurationseinstellungen, um die konfigurierbaren Parameter sowie ihren erwarteten Wert und das erwartete Format anzuzeigen.
   b. Stellen Sie die Parameter ein. Die Werte müssen in dem Bereich liegen, der unter angegeben istKonfigurieren Sie EKS-Add-On-Parameter.
   c. Wählen Sie Änderungen speichern, um das Add-on auf der Grundlage der erweiterten Konfiguration zu erstellen.
   d. Bei der Methode zur Konfliktlösung wird die von Ihnen gewählte Option verwendet, um einen Konflikt zu lösen, wenn Sie den Wert eines Parameters auf einen anderen Wert als den Standardwert aktualisieren. Weitere Informationen zu den aufgelisteten Optionen finden Sie unter ResolveConflicts in der Amazon EKS-API-Referenz.
10. Wählen Sie Weiter aus.
11. Überprüfen Sie auf der Seite Überprüfen und erstellen alle Details und wählen Sie dann Erstellen.
12. Gehen Sie zurück zu den Cluster-Details und wählen Sie die Registerkarte Ressourcen.
13. Sie können die neuen Pods mit dem Präfix aws-guardduty-agent anzeigen.

API/CLI

Sie können den Amazon-EKS-Add-On-Agent (`aws-guardduty-agent`) konfigurieren, indem Sie eine der folgenden Optionen verwenden:

- Renne CreateAddon für dein Konto.

- > **Note**
  >
  > Wenn Sie für das Add-on `version` v1.5.0 oder höher wählen, unterstützt Runtime Monitoring die Konfiguration bestimmter Parameter des GuardDuty Agenten. Weitere Informationen finden Sie unter Konfigurieren Sie EKS-Add-On-Parameter.

  Verwenden Sie die folgenden Werte für die Parameter:

  - Geben Sie unter `addonName` den Wert `aws-guardduty-agent` ein.

    Sie können das folgende AWS CLI Beispiel verwenden, wenn Sie konfigurierbare Werte verwenden, die für Add-On-Versionen `v1.5.0` oder höher unterstützt werden. Stellen Sie sicher, dass Sie die rot hervorgehobenen Platzhalterwerte und die `Example.json` mit den konfigurierten Werten verknüpften Werte ersetzen.

    ```
    aws eks create-addon --region us-east-1 --cluster-name myClusterName --addon-
    name aws-guardduty-agent --addon-version v1.16.0-eksbuild.2 --configuration-
    values 'file://example.json'
    ```

    Example.json

    ```
    {
     "priorityClassName": "aws-guardduty-agent.priorityclass-high",
     "dnsPolicy": "Default",
     "resources": {
      "requests": {
       "cpu": "237m",
       "memory": "512Mi"
      },
      "limits": {
       "cpu": "2000m",
       "memory": "2048Mi"
      }
     }
    }
    ```

  - Weitere Informationen zu unterstützten `addonVersion` finden Sie unter Kubernetes-Versionen, die vom Security Agent unterstützt werden GuardDuty.

- Alternativ können Sie verwenden AWS CLI. Weitere Informationen finden Sie unter create-addon.

Private DNS-Namen für den VPC-Endpunkt

Standardmäßig löst der Security Agent den privaten DNS-Namen des VPC-Endpunkts auf und stellt eine Verbindung zu ihm her. Für einen Nicht-FIPS-Endpunkt wird Ihr privater DNS im folgenden Format angezeigt:

Non-FIPS Endpunkt — `guardduty-data.us-east-1.amazonaws.com`

Das AWS-Region,*us-east-1*, wird sich je nach Ihrer Region ändern.

Manuelles Aktualisieren des Security Agents für Amazon EKS-Ressourcen

Wenn Sie den GuardDuty Security Agent manuell verwalten, sind Sie dafür verantwortlich, ihn für Ihr Konto zu aktualisieren. Um über neue Agentenversionen informiert zu werden, können Sie einen RSS-Feed von abonnierenGuardDuty Release-Versionen des Security Agents.

Sie können den Security Agent auf die neueste Version aktualisieren, um von der zusätzlichen Unterstützung und den Verbesserungen zu profitieren. Wenn Ihre aktuelle Agentenversion das Ende des Standardsupports erreicht, müssen Sie auf eine nächste verfügbare oder die neueste Agentenversion aktualisieren, um Runtime Monitoring (oder EKS Runtime Monitoring) weiterhin verwenden zu können.

Voraussetzung

Bevor Sie die Security Agent-Version aktualisieren, stellen Sie sicher, dass die Agentenversion, die Sie jetzt verwenden möchten, mit Ihrer Kubernetes-Version kompatibel ist. Weitere Informationen finden Sie unter Kubernetes-Versionen, die vom Security Agent unterstützt werden GuardDuty.

Console

1. Öffnen Sie die Amazon EKS-Konsole unter https://console.aws.amazon.com/eks/home #/clusters.
2. Wählen Sie Ihren Clusternamen aus.
3. Wählen Sie unter den Cluster-Informationen die Add-ons Registerkarte aus.

4. Wählen Sie Add-ons auf der Registerkarte GuardDuty EKS Runtime Monitoring aus.
5. Wählen Sie Bearbeiten, um die Agentendetails zu aktualisieren.
6. Aktualisieren Sie auf der Seite „ GuardDuty EKS-Laufzeitüberwachung konfigurieren“ die Details.
7. (Optional) Aktualisierung der optionalen Konfigurationseinstellungen

   Wenn Ihre EKS-Add-On-Version 1.5.0 oder höher ist, können Sie auch das Add-On-Konfigurationsschema aktualisieren.

   a. Erweitern Sie Optionale Konfigurationseinstellungen, um das Konfigurationsschema anzuzeigen.
   b. Aktualisieren Sie die Parameterwerte auf der Grundlage des unter angegebenen BereichsKonfigurieren Sie EKS-Add-On-Parameter.
   c. Wählen Sie Änderungen speichern, um das Update zu starten.
   d. Bei der Konfliktlösungsmethode wird die von Ihnen gewählte Option verwendet, um einen Konflikt zu lösen, wenn Sie den Wert eines Parameters auf einen anderen Wert als den Standardwert aktualisieren. Weitere Informationen zu den aufgelisteten Optionen finden Sie unter ResolveConflicts in der Amazon EKS-API-Referenz.

API/CLI

Informationen zum Aktualisieren des GuardDuty Security Agents für Ihre Amazon EKS-Cluster finden Sie unter Ein Add-on aktualisieren.

> **Note**
>
> Wenn Sie für das Add-on `version` 1.5.0 oder höher wählen, unterstützt Runtime Monitoring die Konfiguration bestimmter Parameter des GuardDuty Agenten. Hinweise zu Parameterbereichen finden Sie unterKonfigurieren Sie EKS-Add-On-Parameter.

Sie können das folgende AWS CLI Beispiel verwenden, wenn Sie konfigurierbare Werte verwenden, die für die Zusatzversionen 1.5.0 und höher unterstützt werden. Stellen Sie sicher, dass Sie die rot hervorgehobenen Platzhalterwerte und die `Example.json` mit den konfigurierten Werten verknüpften Werte ersetzen.

```
aws eks update-addon --region us-east-1 --cluster-name myClusterName --addon-
name aws-guardduty-agent --addon-version v1.16.0-eksbuild.2 --configuration-
values 'file://example.json'
```

Example.json

```
{
 "priorityClassName": "aws-guardduty-agent.priorityclass-high",
 "dnsPolicy": "Default",
 "resources": {
  "requests": {
   "cpu": "237m",
   "memory": "512Mi"
  },
  "limits": {
   "cpu": "2000m",
   "memory": "2048Mi"
  }
 }
}
```

Wenn Ihre Amazon EKS-Add-On-Version 1.5.0 oder höher ist und Sie das Add-On-Schema konfiguriert haben, können Sie überprüfen, ob die Werte für Ihren Cluster korrekt angezeigt werden. Weitere Informationen finden Sie unter Aktualisierungen des Konfigurationsschemas werden überprüft.

Konfigurieren Sie die GuardDuty Security Agent-Parameter (Add-on) für Amazon EKS

Sie können bestimmte Parameter Ihres GuardDuty Security Agents für Amazon EKS konfigurieren. Diese Unterstützung ist für GuardDuty Security Agent Version 1.5.0 und höher verfügbar. Informationen zu den neuesten Add-on-Versionen finden Sie unterGuardDuty Security Agent-Versionen für Amazon EKS-Ressourcen.

Warum sollte ich das Security Agent-Konfigurationsschema aktualisieren

Das Konfigurationsschema für den GuardDuty Security Agent ist für alle Container in Ihren Amazon EKS-Clustern dasselbe. Wenn die Standardwerte nicht mit den zugehörigen Workloads und der Instance-Größe übereinstimmen, sollten Sie erwägen, die CPU-Einstellungen,

Speichereinstellungen und `dnsPolicy` Einstellungen zu konfigurieren. `PriorityClass` Unabhängig davon, wie Sie den GuardDuty Agenten für Ihre Amazon EKS-Cluster verwalten, können Sie die vorhandene Konfiguration dieser Parameter konfigurieren oder aktualisieren.

Automatisiertes Verhalten bei der Agentenkonfiguration mit konfigurierten Parametern

Wenn der Security Agent (EKS-Add-on) in Ihrem Namen GuardDuty verwaltet wird, aktualisiert er das Add-on bei Bedarf. GuardDuty setzt den Wert der konfigurierbaren Parameter auf einen Standardwert. Sie können die Parameter jedoch weiterhin auf einen gewünschten Wert aktualisieren. Wenn dies zu einem Konflikt führt, lautet die Standardoption für ResolveConflicts. `None`

Konfigurierbare Parameter und Werte

Informationen zu den Schritten zur Konfiguration der Zusatzparameter finden Sie unter:

- Manuelles Installieren des GuardDuty Security Agents auf Amazon EKS-Ressourcen oder
- Manuelles Aktualisieren des Security Agents für Amazon EKS-Ressourcen

Die folgenden Tabellen enthalten die Bereiche und Werte, die Sie verwenden können, um das Amazon EKS-Add-on manuell bereitzustellen oder die vorhandenen Add-On-Einstellungen zu aktualisieren.

CPU-Einstellungen

Parameters	Standardwert	Konfigurierbarer Bereich
Anforderungen	200m	Zwischen 200 m und 10000 m, beide inklusive
Einschränkungen	1000m	Zwischen 200 m und 10000 m, beides inklusive
`disableCpuLimits`	`false`	`true` oder `false`

Der `disableCpuLimits` Parameter ist für GuardDuty Security Agent Version 1.12.1-eksbuild.3 und höher verfügbar. In früheren Versionen unterstützt das Add-on diesen Parameter

nicht, und die Amazon EKS-Add-on-APIs (,`UpdateAddon`) geben einen Validierungsfehler zurück`CreateAddon`, wenn Sie ihn angeben.

Wenn Sie `disableCpuLimits` diese Option festlegen`true`, erzwingt der Security Agent-Pod kein CPU-Limit. Andere Ressourceneinstellungen sind nicht betroffen.

Verwenden Sie die folgende Konfiguration, um CPU-Limits zu deaktivieren:

```
{"resources":{"disableCpuLimits":true}}
```

Speicher-Einstellungen

Parameters	Standardwert	Konfigurierbarer Bereich
Anforderungen	256 Mi	Zwischen 256Mi und 20000Mi, beide inklusive
Einschränkungen	1024 Mi	

`PriorityClass`-Einstellungen

Wenn ein Amazon EKS-Add-on für Sie GuardDuty erstellt wird, lautet das zugewiesene`PriorityClass`. `aws-guardduty-agent.priorityclass` Das bedeutet, dass keine Maßnahmen ergriffen werden, die auf der Priorität des Agenten-Pods basieren. Sie können diesen Zusatzparameter konfigurieren, indem Sie eine der folgenden `PriorityClass` Optionen wählen:

Konfigurierbar **`PriorityClass`**	**`preemptionPolicy`** Wert	**`preemptionPolicy`** Beschreibung	Pod-Wert
`aws-guardduty-agent.priorityclass`	`Never`	Keine Aktion	1000000
`aws-guardduty-agent.priorityclass-high`	`PreemptLowerPriority`	Wenn Sie diesen Wert zuweisen, wird verhindert, dass ein Pod mit einem Prioritätswert ausgeführt	100000000

Konfigurierbar **PriorityClass**	**preemptionPolicy** Wert	**preemptionPolicy** Beschreibung	Pod-Wert
`system-cluster-critical` [1]	`PreemptLowerPriority`	wird, der unter dem Pod-Wert des Agenten liegt.	2000000000
`system-node-critical` [1]	`PreemptLowerPriority`		2000001000

[1] Kubernetes bietet diese beiden `PriorityClass` Optionen — und. `system-cluster-critical` `system-node-critical` Weitere Informationen finden Sie PriorityClass in der Kubernetes-Dokumentation.

`dnsPolicy`-Einstellungen

Wählen Sie eine der folgenden DNS-Richtlinienoptionen, die Kubernetes unterstützt. Wenn keine Konfiguration angegeben ist, `ClusterFirst` wird als Standardwert verwendet.

- `ClusterFirst`
- `ClusterFirstWithHostNet`
- `Default`

Informationen zu diesen Richtlinien finden Sie in der DNS-Richtlinie von Pod in der Kubernetes-Dokumentation.

Aktualisierungen des Konfigurationsschemas werden überprüft

Nachdem Sie die Parameter konfiguriert haben, führen Sie die folgenden Schritte aus, um zu überprüfen, ob das Konfigurationsschema aktualisiert wurde:

1. Öffnen Sie die Amazon EKS-Konsole unter https://console.aws.amazon.com/eks/home #/clusters.
2. Klicken Sie im Navigationsbereich auf Cluster.

3. Wählen Sie auf der Seite „Cluster“ den Cluster-Namen aus, für den Sie die Updates überprüfen möchten.
4. Wählen Sie die Registerkarte Resources (Ressourcen) aus.
5. Wählen Sie im Bereich Ressourcentypen unter Workloads die Option aus DaemonSets.
6. Wählen Sie aws-guardduty-agent aus.
7. Wählen Sie auf der Seite aws-guardduty-agent die Raw-Ansicht aus, um die unformatierte JSON-Antwort anzuzeigen. Stellen Sie sicher, dass die konfigurierbaren Parameter den von Ihnen angegebenen Wert anzeigen.

Wechseln Sie nach der Überprüfung zur GuardDuty Konsole. Wählen Sie das entsprechende aus AWS-Region und sehen Sie sich den Abdeckungsstatus für Ihre Amazon EKS-Cluster an. Weitere Informationen finden Sie unter Laufzeitabdeckung und Problembehandlung für Amazon EKS-Cluster.

Validierung der VPC-Endpunktkonfiguration

Nachdem Sie den Security Agent manuell oder über eine GuardDuty automatische Konfiguration installiert haben, können Sie dieses Dokument verwenden, um die VPC-Endpunktkonfiguration zu überprüfen. Sie können diese Schritte auch verwenden, nachdem Sie ein Problem mit der Laufzeitabdeckung für einen Ressourcentyp behoben haben. Sie können sicherstellen, dass die Schritte wie erwartet funktioniert haben und der Abdeckungsstatus möglicherweise als Fehlerfrei angezeigt wird.

Gehen Sie wie folgt vor, um zu überprüfen, ob die VPC-Endpunktkonfiguration für Ihren Ressourcentyp im VPC-Besitzerkonto korrekt eingerichtet ist:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon VPC-Konsole unter. https://console.aws.amazon.com/vpc/
2. Wählen Sie im Navigationsbereich unter Virtual Private Cloud die Option Your VPCs aus.
3. Wählen Sie auf der Seite Ihre VPCs die Option IPv4 CIDR aus, die Ihrer VPC-ID zugeordnet ist.
4. Wählen Sie im Navigationsmenü unter Virtual Private Cloud die Option Endpunkte.
5. Wählen Sie in der Endpoints-Tabelle die Zeile mit dem Servicenamen aus, der com.amazonaws ähnelt. ***us-east-1***.guard-duty-data. Die Region (`us-east-1`) könnte für Ihren Endpunkt unterschiedlich sein.

6. Ein Fenster mit Endpunktdetails wird angezeigt. Wählen Sie auf der Registerkarte „Sicherheitsgruppen“ den Link zur zugehörigen Gruppen-ID aus, um weitere Informationen zu erhalten.
7. Wählen Sie in der Tabelle Sicherheitsgruppen die Zeile mit der zugehörigen Sicherheitsgruppen-ID aus, um die Details anzuzeigen.
8. Stellen Sie auf der Registerkarte „Regeln für eingehenden Verkehr“ sicher, dass es eine Eingangsrichtlinie mit dem Portbereich 443 und der Quelle als Wert gibt, der aus dem IPv4-CIDR kopiert wurde. Eingehende Regeln steuern den eingehenden Datenverkehr, der die Instance erreichen darf. Die folgende Abbildung zeigt die Regeln für eingehenden Datenverkehr für eine Sicherheitsgruppe, die der vom Security Agent verwendete VPC zugeordnet ist. GuardDuty

   Wenn Sie noch keine Sicherheitsgruppe haben, für die ein eingehender Port 443 aktiviert ist, erstellen Sie eine Sicherheitsgruppe im Amazon EC2-Benutzerhandbuch.

   Wenn beim Einschränken der eingehenden Berechtigungen für Ihre VPC (oder Ihren Cluster) ein Problem auftritt, lassen Sie eingehenden Datenverkehr auf Port 443 von einer beliebigen IP-Adresse aus zu (0.0.0. 0/0).

Die folgende Liste enthält wichtige Informationen, die Sie nach der Installation oder Aktualisierung des Security Agents wissen sollten.

Beurteilen Sie die Runtime-Abdeckung

Der nächste Schritt nach der Installation oder Aktualisierung Ihres Security Agents besteht darin, die Runtime-Abdeckung Ihrer Ressourcen zu beurteilen. Wenn der Runtime-Coverage-Status Ungesund lautet, müssen Sie das Problem beheben. Weitere Informationen finden Sie unter Probleme mit der Laufzeitabdeckung und Problembehandlung.

Wenn der Status des Runtime Coverage als Fehlerfrei angezeigt wird, bedeutet dies, dass Runtime Monitoring Runtime-Ereignisse erfassen und empfangen kann. Eine Liste dieser Ereignisse finden Sie unterGesammelte Laufzeit-Ereignistypen.

Privater DNS-Name für den Endpunkt

Nachdem Sie den GuardDuty Security Agent für Ihre Ressourcen installiert haben, löst dieser standardmäßig den privaten DNS-Namen des VPC-Endpunkts auf und stellt eine Verbindung zu ihm her. Für einen Nicht-FIPS-Endpunkt wird das private DNS im folgenden Format angezeigt:

`guardduty-data.us-east-1.amazonaws.com`

Das AWS-Region,*us-east-1*, wird sich je nach Ihrer Region ändern.

Ein Host kann mit zwei Security Agents installiert werden

Wenn Sie mit einem GuardDuty Security Agent für eine Amazon EC2-Instance arbeiten, können Sie den Agenten auf dem zugrunde liegenden Host innerhalb eines Amazon EKS-Clusters installieren und verwenden. Wenn Sie bereits einen Security Agent auf diesem EKS-Cluster bereitgestellt haben, könnten auf demselben Host zwei Security Agents gleichzeitig ausgeführt werden. Informationen zur GuardDuty Funktionsweise in diesem Szenario finden Sie unterSecurity Agents auf demselben Host.

Überprüfung der Statistiken zur Laufzeitabdeckung und Behebung von Problemen

Nachdem Sie Runtime Monitoring aktiviert haben und der GuardDuty Security Agent für Ihre Ressource bereitgestellt wird, GuardDuty werden Abdeckungsstatistiken für den entsprechenden Ressourcentyp und der individuelle Abdeckungsstatus für die Ressourcen angezeigt, die zu Ihrem Konto gehören. Der Deckungsstatus wird bestimmt, indem Sie sicherstellen, dass Sie Runtime Monitoring aktiviert haben, Ihr Amazon VPC-Endpoint erstellt wurde und der GuardDuty Security Agent für die entsprechende Ressource bereitgestellt wurde. Der Coverage-Status „Fehlerhaft“ bedeutet, dass bei einem Laufzeitereignis im Zusammenhang mit Ihrer Ressource das besagte Laufzeitereignis über den Amazon VPC-Endpunkt empfangen und das Verhalten überwacht werden kann. GuardDuty Wenn bei der Konfiguration von Runtime Monitoring, der Erstellung eines Amazon VPC-Endpoints oder der Bereitstellung des GuardDuty Security Agents ein Problem aufgetreten ist, wird der Abdeckungsstatus als Ungesund angezeigt. Wenn der Abdeckungsstatus fehlerhaft ist, können GuardDuty wir das Laufzeitverhalten der entsprechenden Ressource nicht empfangen oder überwachen und auch keine Ergebnisse der Laufzeitüberwachung generieren.

Die folgenden Themen helfen Ihnen dabei, die Abdeckungsstatistiken zu überprüfen, EventBridge Benachrichtigungen zu konfigurieren und die Abdeckungsprobleme für einen bestimmten Ressourcentyp zu beheben.

Inhalt

- Laufzeitabdeckung und Problembehandlung für die Amazon EC2-Instance
- Runtime-Abdeckung und Problembehandlung für Bottlerocket ECS-EC2

- Laufzeitabdeckung und Problembehandlung für Amazon ECS-Cluster
- Laufzeitabdeckung und Problembehandlung für Amazon EKS-Cluster

Laufzeitabdeckung und Problembehandlung für die Amazon EC2-Instance

Für eine Amazon EC2-Ressource wird die Laufzeitabdeckung auf Instance-Ebene bewertet. Ihre Amazon EC2-Instances können unter anderem mehrere Arten von Anwendungen und Workloads in Ihrer Umgebung ausführen. AWS Diese Funktion unterstützt auch von Amazon ECS verwaltete Amazon EC2-Instances. Wenn Sie Amazon ECS-Cluster auf einer Amazon EC2-Instance ausführen, werden die Abdeckungsprobleme auf Instance-Ebene unter Amazon EC2-Runtime Coverage angezeigt.

Themen

- Überprüfen der Abdeckungsstatistiken
- Änderung des Abdeckungsstatus durch Benachrichtigungen EventBridge
- Behebung von Problemen mit der Amazon EC2-Laufzeitabdeckung

Überprüfen der Abdeckungsstatistiken

Die Abdeckungsstatistik für die Amazon EC2-Instances, die Ihren eigenen Konten oder Ihren Mitgliedskonten zugeordnet sind, gibt den Prozentsatz der fehlerfreien EC2-Instances an allen EC2-Instances in der ausgewählten Instanz an. AWS-Region Die folgende Gleichung stellt dies wie folgt dar:

(Fehlerfreie Instanzen) *100 instances/All

Wenn Sie auch den GuardDuty Security Agent für Ihre Amazon ECS-Cluster bereitgestellt haben, wird jedes Problem mit der Abdeckung auf Instance-Ebene im Zusammenhang mit Amazon ECS-Clustern, die auf einer Amazon EC2-Instance ausgeführt werden, als Problem mit der Amazon EC2-Instance-Laufzeit angezeigt.

Wählen Sie eine der Zugriffsmethoden, um die Abdeckungsstatistiken für Ihre Konten einzusehen.

Console

- Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

- Wählen Sie im Navigationsbereich Runtime Monitoring aus.
- Wählen Sie die Registerkarte Runtime Coverage.
- Auf der Registerkarte „EC2-Instance Runtime Coverage“ können Sie die Coverage-Statistiken einsehen, die nach dem Coverage-Status aller Amazon EC2-Instances zusammengefasst sind, die in der Instance-Listentabelle verfügbar sind.
  - Sie können die Instance-Listentabelle nach den folgenden Spalten filtern:
    - Konto-ID
    - Agentenverwaltungs-Typ
    - Version des Agenten
    - Abdeckungsstatus
    - Instanz-ID
    - Cluster-ARN
- Wenn eine Ihrer EC2-Instances den Coverage-Status als Ungesund hat, enthält die Spalte Problem zusätzliche Informationen zum Grund für den Status Ungesund.

API/CLI

- Führen Sie die ListCoverage API mit Ihrer eigenen gültigen Detektor-ID, Ihrer aktuellen Region und Ihrem Service-Endpunkt aus. Mit dieser API können Sie die Instanzliste filtern und sortieren.
  - Sie können das Beispiel `filter-criteria` ändern mit einer der folgenden Optionen für `CriterionKey`:
    - `ACCOUNT_ID`
    - `RESOURCE_TYPE`
    - `COVERAGE_STATUS`
    - `AGENT_VERSION`
    - `MANAGEMENT_TYPE`
    - `INSTANCE_ID`
    - `CLUSTER_ARN`
  - Wenn die `RESOURCE_TYPE` als EC2 **`filter-criteria`** enthalten ist, unterstützt Runtime Monitoring die Verwendung von ISSUE als. `AttributeName` Wenn Sie es verwenden, wird die API-Antwort zu folgendem Ergebnis führen. `InvalidInputException`

Sie können das Beispiel `AttributeName` in `sort-criteria` ändern mit einer der folgenden Optionen:

- `ACCOUNT_ID`
- `COVERAGE_STATUS`
- `INSTANCE_ID`
- `UPDATED_AT`

- Sie können das ändern *`max-results`* (bis zu 50).
- Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
 "EKS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- Führen Sie die GetCoverageStatistics API aus, um aggregierte Statistiken zur Abdeckung abzurufen, die `statisticsType` auf dem basieren.
  - Sie können das Beispiel `statisticsType` zu einer der folgenden Optionen ändern:
    - `COUNT_BY_COVERAGE_STATUS` – Stellt Abdeckungsstatistiken für EKS-Cluster dar, aggregiert nach Abdeckungs-Status.
    - `COUNT_BY_RESOURCE_TYPE`— Abdeckungsstatistiken, aggregiert auf der Grundlage des AWS Ressourcentyps in der Liste.
    - Sie können das Beispiel `filter-criteria` im Befehl ändern. Sie können die folgenden Optionen für `CriterionKey` verwenden:
      - `ACCOUNT_ID`
      - `RESOURCE_TYPE`
      - `COVERAGE_STATUS`
      - `AGENT_VERSION`
      - `MANAGEMENT_TYPE`
      - `INSTANCE_ID`
      - `CLUSTER_ARN`

- Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Wenn der Abdeckungsstatus Ihrer EC2-Instance Ungesund ist, finden Sie weitere Informationen unter. Behebung von Problemen mit der Amazon EC2-Laufzeitabdeckung

Änderung des Abdeckungsstatus durch Benachrichtigungen EventBridge

Der Abdeckungsstatus Ihrer Amazon EC2-Instance wird möglicherweise als Ungesund angezeigt. Um zu erfahren, wann sich der Abdeckungsstatus ändert, empfehlen wir Ihnen, den Abdeckungsstatus regelmäßig zu überwachen und Fehler zu beheben, wenn der Status Ungesund wird. Alternativ können Sie eine EventBridge Amazon-Regel erstellen, um eine Benachrichtigung zu erhalten, wenn sich der Deckungsstatus von Ungesund zu Gesund oder auf andere Weise ändert. Veröffentlichen Sie GuardDuty dies standardmäßig im EventBridge Bus für Ihr Konto.

Beispiel für ein Benachrichtigungsschema

In einer EventBridge Regel können Sie anhand der vordefinierten Beispielereignisse und Ereignismuster eine Benachrichtigung über den Versorgungsstatus erhalten. Weitere Informationen zum Erstellen einer EventBridge Regel finden Sie unter Regel erstellen im EventBridge Amazon-Benutzerhandbuch.

Darüber hinaus können Sie mithilfe des folgenden Beispiel-Benachrichtigungsschemas ein benutzerdefiniertes Ereignismuster erstellen. Achten Sie darauf, die Werte für Ihr Konto zu ersetzen. Um benachrichtigt zu werden, wenn sich der Abdeckungsstatus Ihrer Amazon EC2-Instance von `Healthy` auf ändert`Unhealthy`, `detail-type` sollte der sein*`GuardDuty Runtime Protection Unhealthy`*. Um benachrichtigt zu werden, wenn sich der Abdeckungsstatus von `Unhealthy` zu ändert`Healthy`, ersetzen Sie den Wert von `detail-type` durch*`GuardDuty Runtime Protection Healthy`*.

```
{
  "version": "0",
```

```
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "AWS-Konto ID",
  "time": "event timestamp (string)",
  "region": "AWS-Region",
  "resources": [
       ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "EC2",
        "ec2InstanceDetails": {
          "instanceId":"",
          "instanceType":"",
          "clusterArn": "",
          "agentDetails": {
            "version":""
          },
          "managementType":""
        }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

Behebung von Problemen mit der Amazon EC2-Laufzeitabdeckung

Wenn der Abdeckungsstatus Ihrer Amazon EC2-Instance fehlerhaft ist, können Sie den Grund in der Spalte Problem einsehen.

Wenn Ihre EC2-Instance einem EKS-Cluster zugeordnet ist und der Security Agent für EKS entweder manuell oder über die automatische Agentenkonfiguration installiert wurde, finden Sie Informationen zur Behebung des Abdeckungsproblems unter. Laufzeitabdeckung und Problembehandlung für Amazon EKS-Cluster

In der folgenden Tabelle sind die Problemtypen und die entsprechenden Schritte zur Fehlerbehebung aufgeführt.

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
Keine Agentenberichterstattung	Ich warte auf eine SSM-Benachrichtigung	Das Empfangen der SSM-Benachrichtigung kann einige Minuten dauern. Stellen Sie sicher, dass die Amazon EC2-Instance SSM-verwaltet wird. Weitere Informationen finden Sie in den Schritten unter Methode 1 — Mithilfe des AWS Systems Managers unter. Manuelles Installieren des Security Agents
	(Absichtlich leer)	Wenn Sie den GuardDuty Security Agent manuell verwalten, stellen Sie sicher, dass Sie die Schritte unter befolgt habenManuelles Verwalten des Security Agents für die Amazon EC2-Ressource.
		Wenn Sie die automatische Agentenkonfiguration aktiviert haben: • Ihre EC2-Instance wird von SSM verwaltet. • Sehen Sie sich regelmäßig den Status Ihres Security Agents an. Weitere Informationen finden Sie unter Überprüfung des Installat

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
		ionsstatus des GuardDuty Security Agents.
		Stellen Sie sicher, dass der VPC-Endpunkt für Ihre Amazon EC2-Instance korrekt konfiguriert ist. Weitere Informationen finden Sie unter Validierung der VPC-Endpunktkonfiguration.
		Wenn Ihre Organisation über eine Service Control Policy (SCP) verfügt, stellen Sie sicher, dass die Berechtigungsgrenze die Berechtigung nicht einschränkt. `guardduty:SendSecurityTelemetry` Weitere Informationen finden Sie unter Validierung der Service Control-Richtlinie Ihres Unternehmens in einer Umgebung mit mehreren Konten.

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
	Die Verbindung zum Agenten wurde unterbrochen	• Sehen Sie sich den Status Ihres Security Agents an. Weitere Informationen finden Sie unter Überprüfung des Installationsstatus des GuardDuty Security Agents. • Sehen Sie sich die Security Agent-Protokolle an, um die potenzielle Ursache zu ermitteln. Die Protokolle enthalten detaillierte Fehler, anhand derer Sie das Problem selbst beheben können. Die Protokolldateien sind unter verfügbar `/var/log/amzn-guardduty-agent/` . `Tsudo journalctl -u amazon-guardduty-agent .`
Agent wurde nicht bereitgestellt	Instanzen mit Ausschluss-Tags sind von Runtime Monitoring ausgeschlossen.	GuardDuty empfängt keine Laufzeitereignisse von Amazon EC2-Instances, die mit dem Ausschluss-Tag`GuardDutyManaged : false` gestartet werden. Um Laufzeitereignisse von dieser Amazon EC2-Instance zu empfangen, entfernen Sie das Ausschluss-Tag.

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
	Die Kernel-Version ist niedriger als die unterstützte Version.	Informationen zu den unterstützten Kernelversionen aller Betriebssystemverteilungen finden Sie unter Überprüfen Sie die architektonischen Anforderungen für Amazon EC2-Instances.
	Die Kernel-Version ist höher als die unterstützte Version.	Informationen zu den unterstützten Kernelversionen aller Betriebssystemverteilungen finden Sie unter Überprüfen Sie die architektonischen Anforderungen für Amazon EC2-Instances.

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
	Das Identitätsdokument für die Instanz konnte nicht abgerufen werden.	Dazu gehen Sie wie folgt vor: 1. Vergewissern Sie sich, dass es sich bei Ihrer Ressource um eine Amazon EC2-Instance und nicht um eine Hybrid-Instance handelt, die nicht von EC2 stammt. 2. Vergewissern Sie sich, dass der Instance Metadata Service (IMDS) aktiviert ist. Informationen dazu finden Sie im Amazon EC2-Benutzerhandbuch unter Konfigurieren der Optionen für den Instance Metadata Service. 3. Stellen Sie sicher, dass das Instanz-Identitäts dokument existiert. Informationen dazu finden Sie im Amazon EC2-Benutzerhandbuch unter Abrufen des Instance-Identitätsdokuments. 4. Wenn das Instanz-Identitäts dokument immer noch nicht existiert, starten Sie die Instance neu. Das Instance-Identitätsdokument wird generiert, wenn die Instance angehalten und gestartet, neu gestartet oder gelauncht wird.

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
Die Erstellung der SSM-Zuordnung ist fehlgeschlagen	GuardDuty Die SSM-Zuordnung ist bereits in Ihrem Konto vorhanden	1. Löschen Sie die bestehende Verknüpfung manuell. Weitere Informationen finden Sie im AWS Systems Manager Benutzerhandbuch unter Löschen von Verknüpfungen. 2. Nachdem Sie die Zuordnung gelöscht haben, deaktivieren Sie die GuardDuty automatische Agentenkonfiguration für Amazon EC2 und aktivieren Sie sie erneut.
	Ihr Konto hat zu viele SSM-Verknüpfungen	Wählen Sie eine der folgenden beiden Optionen: • Löschen Sie alle unbenutzten SSM-Zuordnungen. Weitere Informationen finden Sie im AWS Systems Manager Benutzerhandbuch unter Löschen von Zuordnungen. • Prüfen Sie, ob Ihr Konto für eine Kontingenterhöhung in Frage kommt. Weitere Informationen finden Sie unter Systems Manager Service-Kontingente im Allgemeine AWS-Referenz.

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
Die Aktualisierung der SSM-Zuordnung ist fehlgeschlagen	GuardDuty Die SSM-Zuordnung ist in Ihrem Konto nicht vorhanden	GuardDuty Die SSM-Zuordnung ist in Ihrem Konto nicht vorhanden. Deaktivieren Sie Runtime Monitoring und aktivieren Sie es erneut.
Das Löschen der SSM-Zuordnung ist fehlgeschlagen	GuardDuty Die SSM-Zuordnung ist in Ihrem Konto nicht vorhanden	Die SSM-Vereinigung ist in Ihrem Konto nicht vorhanden . Wenn die SSM-Zuordnung absichtlich gelöscht wurde, ist keine Aktion erforderlich.

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
Die Ausführung der SSM-Instanzzuordnung ist fehlgeschlagen	Die architektonischen Anforderungen oder andere Voraussetzungen sind nicht erfüllt.	Hinweise zu verifizierten Betriebssystemverteilungen finden Sie unterVoraussetzungen für die Unterstützung von Amazon EC2-Instances. Wenn dieses Problem weiterhin auftritt, helfen Ihnen die folgenden Schritte dabei, das Problem zu identifizieren und möglicherweise zu lösen: 1. Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/. 2. Wählen Sie im Navigationsbereich unter Node Management die Option State Manager aus. 3. Filtern Sie nach der Eigenschaft „Dokumentname“ und geben Sie Folgendes ein AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin. 4. Wählen Sie die entsprechende Assoziations-ID aus und sehen Sie sich den Ausführungsverlauf an. 5. Sehen Sie sich anhand des Ausführungsverlauf

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
		s die Fehler an, identifiz ieren Sie die mögliche Grundursache und versuchen Sie, sie zu beheben.
Die Erstellung des VPC-Endpo ints ist fehlgeschlagen	Die Erstellung von VPC-Endpu nkten wird für gemeinsam genutzte VPC nicht unterstützt *vpcId*	Runtime Monitoring unterstüt zt die Verwendung einer gemeinsam genutzten VPC innerhalb einer Organisation. Weitere Informationen finden Sie unter Verwenden von gemeinsam genutzter VPC mit Runtime Monitoring.
	Nur bei Verwendung einer gemeinsam genutzten VPC mit automatisierter Agentenko nfiguration Für die Inhaber-Konto-ID *111122223333* für eine gemeinsam genutzte VPC *vpcId* ist weder Runtime Monitoring noch automatische Agentenkonfiguration oder beides aktiviert	Das gemeinsame VPC-Besit zerkonto muss Runtime Monitoring und automatis che Agentenkonfigurati on für mindestens einen Ressourcentyp (Amazon EKS oder Amazon ECS (AWS Fargate)) aktivieren. Weitere Informationen finden Sie unter Spezifische Vorausset zungen für Runtime Monitoring GuardDuty.

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
	Für die Aktivierung von privatem DNS müssen beide `enableDnsSupport` `enableDnsHostnames` VPC-Attribute auf `true` for *`vpcId`* (Service: Ec2, Status Code:400, Request-ID:) gesetzt sein. *`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`*	Sie müssen jedoch sicherstellen, dass die folgenden VPC-Attribute auf `true` festgelegt sind: `enableDnsSupport` und `enableDnsHostnames` . Weitere Informationen finden Sie unter DNS-Attribute in Ihrer VPC. Wenn Sie Amazon VPC Console unter verwenden, um die Amazon VPC https://console.aws.amazon.com/vpc/ zu erstellen, wählen Sie sowohl DNS-Hostnamen aktivieren als auch DNS-Auflösung aktivieren aus. Weitere Informationen finden Sie unter VPC-Konfigurationsoptionen. Nach der Aktualisierung der VPC-Attribute müssen Sie die Erstellung des VPC-Endpoints beschleunigen, indem Sie eine der folgenden Änderungen vornehmen: • Sie können das `GuardDutyManaged` Tag für Ihre Amazon EC2-Instance hinzufügen oder ändern (empfohlen). Sie können beispielsweise hinzufügen `GuardDutyManaged` :, `true` um die Instance

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
		für Runtime Monitoring einzubeziehen. • Sie können den Status der Amazon EC2-Instance ändern (stoppen oder neu starten).

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
Das Löschen des gemeinsamen VPC-Endpoints ist fehlgeschlagen	Das Löschen eines gemeinsamen VPC-Endpunkts für Konto-ID *111122223333* , gemeinsame VPC *vpcId* und Besitzerkonto-ID ist nicht zulässig. *555555555555*	Mögliche Schritte: • Die Deaktivierung des Runtime Monitoring-Status des gemeinsam genutzten VPC-Teilnehmerkontos hat keine Auswirkungen auf die gemeinsame VPC-Endpunktrichtlinie und die Sicherheitsgruppe, die im Besitzerkonto vorhanden ist. Um den gemeinsam genutzten VPC-Endpoint und die Sicherheitsgruppe zu löschen, müssen Sie Runtime Monitoring oder den automatisierten Agent-Konfigurationsstatus im gemeinsam genutzten VPC-Besitzerkonto deaktivieren. • Das gemeinsame VPC-Teilnehmerkonto kann den gemeinsam genutzten VPC-Endpunkt und die Sicherheitsgruppe, die im gemeinsamen VPC-Besit zerkonto gehostet werden, nicht löschen.

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
Der Agent meldet sich nicht	(Absichtlich leer)	Der Support für diesen Problemtyp ist abgelaufe n. Wenn dieses Problem weiterhin auftritt und noch nicht geschehen ist, aktivieren Sie den GuardDuty automatis ierten Agenten für Amazon EC2. Wenn das Problem weiterhin besteht, sollten Sie in Erwägung ziehen, Runtime Monitoring für einige Minuten zu deaktivieren und dann erneut zu aktivieren.

Runtime-Abdeckung und Problembehandlung für Bottlerocket ECS-EC2

Evaluiert für Bottlerocket Amazon EC2-Instances in Amazon ECS-Clustern die Laufzeitabdeckung auf Instance-Ebene. GuardDuty Der GuardDuty Security Agent läuft als Host-Container auf Bottlerocket und nicht als installiertes RPM- oder Debian-Paket.

Bottlerocket Amazon EC2-Instances werden auf der Registerkarte EC2-Instance-Runtime Coverage angezeigt. Um die Abdeckungsstatistiken für Ihre Bottlerocket-Instances zu überprüfen, öffnen Sie die GuardDuty Konsole, wählen Sie im Navigationsbereich Runtime Monitoring aus und wählen Sie dann die Registerkarte Runtime Coverage. Unter EC2-Instance Runtime Coverage können Sie den Coverage-Status jeder Instance einsehen und nach Konto-ID, Agentenversion oder Coverage-Status filtern. Weitere Informationen finden Sie unter Überprüfen der Abdeckungsstatistiken.

Behebung von Problemen mit der Bottlerocket-Runtime-Abdeckung ECS-EC2

Wenn der Abdeckungsstatus Ihrer Bottlerocket Amazon EC2-Instance fehlerhaft ist, können Sie den Grund in der Spalte Problem einsehen.

In der folgenden Tabelle sind die Problemtypen und die entsprechenden Schritte zur Fehlerbehebung aufgeführt.

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
Keine Agentenberichterstattung	Ich warte auf eine SSM-Benachrichtigung	Das Empfangen der SSM-Benachrichtigung kann einige Minuten dauern. Stellen Sie sicher, dass Ihre Bottlerocket-Instanz SSM-verwaltet wird. Der SSM-Agent wird standardmäßig im Bottlerocket Control-Container ausgeführt. Stellen Sie sicher, dass das Instanzprofil die und verwalteten Richtlinien enthält. `AmazonSSMManagedInstanceCore` `AmazonEC2ContainerRegistryReadOnly`
Keine Agentenberichterstattung	Nicht zutreffend	Stellen Sie sicher, dass der Agent-Host-Container aktiviert ist und läuft: 1. Stellen Sie mithilfe des SSM Session Managers eine Verbindung zu Ihrer Instance her. 2. Geben Sie den Admin-Container ein:`enter-admin-container` . 3. Einstellungen überprüfen:`apiclient get settings.host-containers.amazon-guardduty-agent` . Bestätigen Sie, dass

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
		`enabled` das ist `true` und `superpowered` ist`true`. 4. Überprüfen Sie, ob der Agentenprozess läuft:`sheltie ps aux | grep guardduty` . 5. Überprüfen Sie die Agentenprotokolle mit einer der folgenden Methoden: • `sheltie journalctl -u host-containers@amazon-guardduty-agent` • Aus einer Sheltie-Sitzung (`sudo sheltie`):`ls /var/log/amzn-guardduty-agent/` .
Keine Agentenberichterstattung	Nicht zutreffend	Stellen Sie sicher, dass die Instance über eine Netzwerkkonnektivität zum Amazon ECR-Endpunkt und zum GuardDuty VPC-Endpunkt verfügt. Wenn Ihre Instance in einem privaten Subnetz ausgeführt wird, stellen Sie sicher, dass Sie VPC-Endpunkte sowohl für Amazon ECR als auch konfiguriert haben. GuardDuty

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
Keine Agentenberichterstattung	Nicht zutreffend	Wenn Ihre Organisation über eine Service Control Policy (SCP) verfügt, stellen Sie sicher, dass die Berechtigungsgrenze diese `guardduty:SendSecurityTelemetry` Genehmigung zulässt.
Die Erstellung der SSM-Zuordnung ist fehlgeschlagen	GuardDuty Die SSM-Zuordnung ist bereits in Ihrem Konto vorhanden.	1. Löschen Sie die bestehende Verknüpfung manuell. Weitere Informationen finden Sie im AWS Systems Manager Benutzerhandbuch unter Löschen von Verknüpfungen. 2. Nachdem Sie die Zuordnung gelöscht haben, deaktivieren Sie die GuardDuty automatische Agentenkonfiguration für Amazon EC2 und aktivieren Sie sie erneut.

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
Die Erstellung der SSM-Zuordnung ist fehlgeschlagen	Ihr Konto hat zu viele SSM-Verknüpfungen.	Wählen Sie eine der folgenden beiden Optionen: • Löschen Sie alle unbenutzten SSM-Zuordnungen. Weitere Informationen finden Sie im AWS Systems Manager Benutzerhandbuch unter Löschen von Zuordnungen. • Prüfen Sie, ob Ihr Konto für eine Kontingenterhöhung in Frage kommt. Weitere Informationen finden Sie unter Systems Manager Service-Kontingente im Allgemeine AWS-Referenz.
SSM-Zuordnungsupdate fehlgeschlagen	GuardDuty Die SSM-Zuordnung ist in Ihrem Konto nicht vorhanden.	GuardDuty Die SSM-Zuordnung ist in Ihrem Konto nicht vorhanden. Deaktivieren Sie Runtime Monitoring und aktivieren Sie es erneut.
Das Löschen der SSM-Zuordnung ist fehlgeschlagen	GuardDuty Die SSM-Zuordnung ist in Ihrem Konto nicht vorhanden.	Die SSM-Vereinigung ist in Ihrem Konto nicht vorhanden . Wenn die SSM-Zuordnung absichtlich gelöscht wurde, ist keine Aktion erforderlich.

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
Die Ausführung der SSM-Instanzzuordnung ist fehlgeschlagen	Die architektonischen Anforderungen oder andere Voraussetzungen sind nicht erfüllt.	Informationen zu verifizierten Anforderungen finden Sie unterVoraussetzungen für die ECS-EC2 Bottlerocket-Unterstützung. Wenn dieses Problem weiterhin auftritt, überprüfen Sie den Ausführungsverlauf von SSM State Manager: 1. Öffnen Sie die AWS Systems Manager Konsole unter. https://console.aws.amazon.com/systems-manager/ 2. Wählen Sie im Navigationsbereich unter Node Management die Option State Manager aus. 3. Filtern Sie nach der Eigenschaft „Dokumentname“ und geben Sie Folgendes ein AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin. 4. Wählen Sie die entsprechende Assoziations-ID aus und sehen Sie sich den Ausführungsverlauf an. 5. Sehen Sie sich anhand des Ausführungsverlaufs die Fehler an, identifiz

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
		ieren Sie die mögliche Grundursache und versuchen Sie, sie zu beheben.
Die Verbindung zum Agenten wurde unterbrochen	Nicht zutreffend	• Überprüfen Sie die Agentenprotokolle im Admin-Container: `enter-admin-container sheltie journalctl -u host-containers@amazon-guardduty-agent` • Stellen Sie sicher, dass das Agent-Container-Image erfolgreich abgerufen wurde, indem Sie überprüfen, ob das `source` Feld in den Host-Container-Einstellungen auf eine gültige Amazon ECR-URI verweist. • Stellen Sie sicher, dass das Instanzprofil über Amazon ECR-Pull-Berechtigungen verfügt. Weitere Informationen finden Sie unter Sorgen Sie dafür, dass EC2-Instances von SSM verwaltet werden, und konfigurieren Sie Instance-Berechtigungen.

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
Agent wurde nicht bereitgestellt	Instanzen mit Ausschluss-Tags sind von Runtime Monitoring ausgeschlossen.	GuardDuty empfängt keine Laufzeitereignisse von Amazon EC2-Instances, die mit dem Ausschluss-Tag `GuardDutyManaged : false` gestartet werden. Um Laufzeitereignisse von dieser Instance zu empfangen, entfernen Sie das Ausschluss-Tag.
Agent wurde nicht bereitgestellt	Die Kernel-Version ist niedriger als die unterstützte Version.	Aktualisieren Sie für die automatische Agentenkonfiguration auf das neueste Bottlerocket `v1.62.1` - ECS-2 oder ECS-3 optimierte AMI oder höher.

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
Der Abruf des ECR-Images ist fehlgeschlagen	Das Agent-Container-Image konnte nicht aus Amazon ECR abgerufen werden.	• Stellen Sie sicher, dass das Instanzprofil eine `AmazonEC2ContainerRegistryReadOnly` verwaltete Richtlinie oder die erforderlichen individuellen Amazon ECR-Berechtigungen enthält. • Überprüfen Sie die Netzwerkkonnektivität zum Amazon ECR-Endpunkt in Ihrer Region. • Wenn Sie ein privates Subnetz verwenden, stellen Sie sicher, dass die VPC-Endpunkte konfiguriert sind. Weitere Informationen finden Sie unter Anforderungen an die Netzwerkkonnektivität.

Laufzeitabdeckung und Problembehandlung für Amazon ECS-Cluster

Die Laufzeitabdeckung für Amazon ECS-Cluster umfasst die Aufgaben, die auf AWS Fargate Amazon ECS-Container-Instances ausgeführt werden [1].

Bei einem Amazon ECS-Cluster, der auf Fargate ausgeführt wird, wird die Laufzeitabdeckung auf Aufgabenebene bewertet. Die ECS-Cluster-Laufzeitabdeckung umfasst die Fargate-Aufgaben, die ausgeführt wurden, nachdem Sie die Laufzeitüberwachung und die automatische Agentenkonfiguration für Fargate aktiviert haben (nur ECS). Standardmäßig ist eine Fargate-Aufgabe unveränderlich. GuardDuty wird nicht in der Lage sein, den Security Agent zur Überwachung von Containern auf bereits laufenden Aufgaben zu installieren. Um eine solche Fargate-Aufgabe einzubeziehen, müssen Sie die Aufgabe beenden und erneut starten. Prüfen Sie unbedingt, ob der zugehörige Dienst unterstützt wird.

Informationen zum Amazon ECS-Container finden Sie unter Kapazitätserstellung.

Inhalt

- Überprüfen der Abdeckungsstatistiken
- Änderung des Deckungsstatus durch EventBridge Benachrichtigungen
- Behebung von Problemen mit der ECS-Fargate Amazon-Laufzeitabdeckung

Überprüfen der Abdeckungsstatistiken

Die Abdeckungsstatistik für die Amazon ECS-Ressourcen, die Ihrem eigenen Konto oder Ihren Mitgliedskonten zugeordnet sind, entspricht dem Prozentsatz der intakten Amazon ECS-Cluster an allen Amazon ECS-Clustern in den ausgewählten AWS-Region. Dies beinhaltet die Abdeckung für Amazon ECS-Cluster, die sowohl Fargate- als auch Amazon EC2-Instances zugeordnet sind. Die folgende Gleichung stellt dies wie folgt dar:

(Fehlerfreie clusters/All Cluster) *100

Überlegungen

- Die Abdeckungsstatistiken für den ECS-Cluster beinhalten den Abdeckungsstatus der Fargate-Aufgaben oder ECS-Container-Instances, die diesem ECS-Cluster zugeordnet sind. Der Abdeckungsstatus der Fargate-Aufgaben umfasst Aufgaben, die sich entweder im Status „Running“ befinden oder vor Kurzem abgeschlossen wurden.
- Auf der Registerkarte „ECS-Cluster-Laufzeitabdeckung“ gibt das Feld „Abgedeckte Container-Instances“ den Abdeckungsstatus der Amazon EC2-Container-Instances an, die Ihrem Amazon ECS-Cluster zugeordnet sind.

  Wenn auf Ihrem Amazon ECS-Cluster nur der Starttyp Fargate ausgeführt wird, wird in diesem Feld ein Bindestrich (-) angezeigt, um anzuzeigen, dass die Anzahl nicht zutrifft. Ein Fargate-only Cluster muss keine Amazon EC2-Container-Instances abdecken.
- Wenn Ihr Amazon ECS-Cluster mit einer Amazon EC2-Instance verknüpft ist, die über keinen Sicherheitsagenten verfügt, weist der Amazon ECS-Cluster ebenfalls den Status Ungesund auf.

  Informationen zur Identifizierung und Behebung des Abdeckungsproblems für die zugehörige Amazon EC2-Instance finden Sie unter Behebung von Problemen mit der Amazon EC2-Laufzeitabdeckung für Amazon EC2-Instances.

Wählen Sie eine der Zugriffsmethoden, um die Abdeckungsstatistiken für Ihre Konten einzusehen.

Console

- Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/
- Wählen Sie im Navigationsbereich Runtime Monitoring aus.
- Wählen Sie die Registerkarte Runtime Coverage.
- Auf der Registerkarte ECS-Cluster-Laufzeitabdeckung können Sie die Abdeckungsstatistiken einsehen, die nach dem Abdeckungsstatus jedes Amazon ECS-Clusters zusammengefasst sind, der in der Cluster-Listentabelle verfügbar ist.
  - Sie können die Cluster-Listentabelle nach den folgenden Spalten filtern:
    - Konto-ID
    - Cluster-Name
    - Agentenverwaltungs-Typ
    - Abdeckungsstatus
- Wenn einer Ihrer Amazon ECS-Cluster den Deckungsstatus Ungesund hat, enthält die Spalte Problem zusätzliche Informationen über den Grund für den Status Ungesund.

  Wenn Ihre Amazon ECS-Cluster mit einer Amazon EC2-Instance verknüpft sind, navigieren Sie zur Registerkarte EC2-Instance Runtime Coverage und filtern Sie nach dem Feld Clustername, um das zugehörige Problem anzuzeigen.

API/CLI

- Führen Sie die ListCoverage API mit Ihrer eigenen gültigen Detektor-ID, Ihrer aktuellen Region und Ihrem Service-Endpunkt aus. Mit dieser API können Sie die Instanzliste filtern und sortieren.
  - Sie können das Beispiel `filter-criteria` ändern mit einer der folgenden Optionen für `CriterionKey`:
    - `ACCOUNT_ID`
    - `ECS_CLUSTER_NAME`
    - `COVERAGE_STATUS`
    - `MANAGEMENT_TYPE`

- Sie können das Beispiel `AttributeName` in `sort-criteria` ändern mit einer der folgenden Optionen:
  - `ACCOUNT_ID`
  - `COVERAGE_STATUS`
  - `ISSUE`
  - `ECS_CLUSTER_NAME`
  - `UPDATED_AT`

    Das Feld wird nur aktualisiert, wenn entweder eine neue Aufgabe im zugehörigen Amazon ECS-Cluster erstellt wird oder sich der entsprechende Abdeckungsstatus ändert.
- Sie können den ändern *`max-results`* (bis zu 50).
- Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
 "ECS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- Führen Sie die GetCoverageStatistics API aus, um aggregierte Statistiken zur Abdeckung abzurufen, die `statisticsType` auf dem basieren.
  - Sie können das Beispiel `statisticsType` zu einer der folgenden Optionen ändern:
    - `COUNT_BY_COVERAGE_STATUS`— Stellt Abdeckungsstatistiken für ECS-Cluster dar, die nach dem Abdeckungsstatus aggregiert sind.
    - `COUNT_BY_RESOURCE_TYPE`— Abdeckungsstatistiken, aggregiert auf der Grundlage des AWS Ressourcentyps in der Liste.
    - Sie können das Beispiel `filter-criteria` im Befehl ändern. Sie können die folgenden Optionen für `CriterionKey` verwenden:
      - `ACCOUNT_ID`
      - `ECS_CLUSTER_NAME`
      - `COVERAGE_STATUS`
      - `MANAGEMENT_TYPE`

    - `INSTANCE_ID`
- Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Weitere Informationen zu Deckungsproblemen finden Sie unterBehebung von Problemen mit der ECS-Fargate Amazon-Laufzeitabdeckung.

Änderung des Deckungsstatus durch EventBridge Benachrichtigungen

Der Abdeckungsstatus Ihres Amazon ECS-Clusters wird möglicherweise als Ungesund angezeigt. Um zu erfahren, wann sich der Abdeckungsstatus ändert, empfehlen wir Ihnen, den Abdeckungsstatus regelmäßig zu überwachen und Fehler zu beheben, wenn der Status Ungesund wird. Alternativ können Sie eine EventBridge Amazon-Regel erstellen, um eine Benachrichtigung zu erhalten, wenn sich der Deckungsstatus von Ungesund zu Gesund oder auf andere Weise ändert. Veröffentlichen Sie GuardDuty dies standardmäßig im EventBridge Bus für Ihr Konto.

Beispiel für ein Benachrichtigungsschema

In einer EventBridge Regel können Sie anhand der vordefinierten Beispielereignisse und Ereignismuster eine Benachrichtigung über den Versorgungsstatus erhalten. Weitere Informationen zum Erstellen einer EventBridge Regel finden Sie unter Regel erstellen im EventBridge Amazon-Benutzerhandbuch.

Darüber hinaus können Sie mithilfe des folgenden Beispiel-Benachrichtigungsschemas ein benutzerdefiniertes Ereignismuster erstellen. Achten Sie darauf, die Werte für Ihr Konto zu ersetzen. Um benachrichtigt zu werden, wenn sich der Abdeckungsstatus Ihres Amazon ECS-Clusters von `Healthy` auf ändert`Unhealthy`, `detail-type` sollte *`GuardDuty Runtime Protection Unhealthy`* der Um benachrichtigt zu werden, wenn sich der Abdeckungsstatus von `Unhealthy` zu ändert`Healthy`, ersetzen Sie den Wert von `detail-type` durch*`GuardDuty Runtime Protection Healthy`*.

```
{
```

```
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "AWS-Konto ID",
  "time": "event timestamp (string)",
  "region": "AWS-Region",
  "resources": [
       ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "ECS",
        "ecsClusterDetails": {
          "clusterName":"",
          "fargateDetails":{
            "issues":[],
            "managementType":""
          },
          "containerInstanceDetails":{
            "coveredContainerInstances":int,
            "compatibleContainerInstances":int
          }
        }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

Behebung von Problemen mit der ECS-Fargate Amazon-Laufzeitabdeckung

Wenn der Abdeckungsstatus Ihres Amazon ECS-Clusters fehlerhaft ist, können Sie den Grund in der Spalte Problem einsehen.

Die folgende Tabelle enthält die empfohlenen Schritte zur Fehlerbehebung bei Fargate-Problemen (nur Amazon ECS). Informationen zu Problemen mit der Abdeckung durch Amazon EC2-Instances finden Sie unter Behebung von Problemen mit der Amazon EC2-Laufzeitabdeckung für Amazon EC2-Instances.

Art des Problems	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
Der Agent meldet sich nicht		Stellen Sie sicher, dass der VPC-Endpunkt für die Aufgabe Ihres Amazon ECS-Clusters korrekt konfiguriert ist. Weitere Informationen finden Sie unter Validierung der VPC-Endpunktkonfiguration.
	Der Agent meldet sich nicht für Aufgaben in `TaskDefinition - ' TASK_DEFINITION '`	Wenn Ihre Organisation über eine Service Control Policy (SCP) verfügt, stellen Sie sicher, dass die Berechtigungsgrenze die Berechtigungen nicht einschränkt. `guardduty:SendSecurityTelemetry` Weitere Informationen finden Sie unter Validierung der Service Control-Richtlinie Ihres Unternehmens in einer Umgebung mit mehreren Konten.
	`VPC_ISSUE ; for task in TaskDefinition - 'TASK_DEFINITION '`	Die Details zum VPC-Problem finden Sie in den zusätzlichen Informationen.
Der Agent wurde beendet	ExitCode: `EXIT_CODE` für Aufgaben in `TaskDefinition - ' TASK_DEFINITION '`	Sehen Sie sich die Problemdetails in den zusätzlichen Informationen an.

Art des Problems	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
	Grund: *REASON* für Aufgaben in `TaskDefinition - '`*TASK_DEFINITION*` '`	
	ExitCode: `EXIT_CODE` mit Grund: '*EXIT_CODE* ' für Aufgaben in `TaskDefinition - '` *TASK_DEFINITION* '	

Art des Problems	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
	Agent wurde beendet: GrundCannotPullContainerError : Der Abruf des Image-Manifests wurde erneut versucht...	In diesem Szenario kann GuardDuty das Sidecar-Container-Image möglicherweise nicht abgerufen werden. Ihre Aufgabe wird weiterhin ausgeführt, GuardDuty kann jedoch keine potenziellen Bedrohungen erkennen. Führen Sie nacheinander die folgenden Schritte zur Fehlerbehebung durch, um zu überprüfen, ob dies zur Lösung des Netzabdeckungsproblems beiträgt: • Berechtigungen: Stellen Sie sicher, dass Ihre Rolle zur Aufgabenausführung über die erforderlichen ECR-Berechtigungen verfügt, die unter aufgeführt sind. Berechtigungsanforderungen • Netzwerkkonnektivität: Stellen Sie sicher, dass Ihre Fargate-Aufgaben ECR entweder über einen öffentlichen Internetzugang oder über ordnungsgemäß konfigurierte VPC-Endpunkte erreichen können, wie unter beschrieben. Anforderungen an die Netzwerkkonnektivität

Art des Problems	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
		• Konfiguration der Sicherheitsgruppe: Stellen Sie sicher, dass Ihre Sicherheitsgruppe den ausgehenden Zugriff auf die verwaltete S3-Präfixliste auf Port 443 zulässt, wie unter beschrieben. Sicherheitsgruppenkonfiguration • Führen Sie das AWSSupport-TroubleshootECSTaskFailedToStart Runbook in der Region Ihres Clusters aus, um bestimmte Probleme zu identifizieren. • In den Aufgabenprotokollen finden Sie Fehlermeldungen. Informationen dazu finden Sie unter Anzeigen von Amazon ECS-Container-Agent-Protokollen im Amazon Elastic Container Service Developer Guide. Informationen zu häufigen Fehlern und zur Problembehandlung finden Sie unter Amazon ECS-Fehlerbehebung im Amazon Elastic Container Service Developer Guide.

Art des Problems	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
		Diese drei Komponenten (Berechtigungen, Netzwerkkonnektivität und Sicherheitsgruppenkonfiguration) sind unabhängig, aber alle erforderlich, um das GuardDuty Container-Image erfolgreich von Amazon ECR herunterzuladen. Wenn das Problem weiterhin besteht, finden Sie weitere Informationen unter. Mein AWS Step Functions Workflow schlägt unerwartet fehl

Art des Problems	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
Die Erstellung des VPC-Endpoints ist fehlgeschlagen	Für die Aktivierung von privatem DNS müssen beide `enableDnsSupport` `enableDnsHostnames` VPC-Attribute auf `true` for *`vpcId`* (Service: EC2, Status Code:400, Request-ID:) gesetzt sein. *`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`*	Sie müssen jedoch sicherstellen, dass die folgenden VPC-Attribute auf `true` festgelegt sind: `enableDnsSupport` und `enableDnsHostnames` . Weitere Informationen finden Sie unter DNS-Attribute in Ihrer VPC. Wenn Sie Amazon VPC Console unter verwenden, um die Amazon VPC https://console.aws.amazon.com/vpc/ zu erstellen, stellen Sie sicher, dass Sie sowohl DNS-Hostnamen aktivieren als auch DNS-Auflösung aktivieren auswählen. Weitere Informationen finden Sie unter VPC-Konfigurationsoptionen.
	Der Aufruf von *`SERVICE`* vier Aufgabe (n) in wird nicht unterstützt `TaskDefinition - '` *`TASK_DEFINITION`* `'`	Diese Aufgabe wurde von einer aufgerufen*`SERVICE`*, die nicht unterstützt wird.
Der Agent wurde nicht bereitgestellt	Die CPU-Architektur '*`TYPE`*' wird für Aufgabe (n) in nicht unterstützt `TaskDefinition - '` *`TASK_DEFINITION`* `'`	Diese Aufgabe wird auf einer nicht unterstützten CPU-Architektur ausgeführt. Hinweise zu unterstützten CPU-Architekturen finden Sie unter. Validierung der architektonischen Anforderungen

Art des Problems	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
	`TaskExecutionRole` fehlt von `TaskDefinition - '`*`TASK_DEFINITION`*` '`	Die Rolle zur Ausführung der ECS-Aufgabe fehlt. Hinweise zur Bereitstellung der Rolle zur Aufgabenausführung und zu den erforderlichen Berechtigungen finden Sie unterVoraussetzungen für den Zugriff auf Container-Images.
	Fehlende Netzwerkkonfiguration *`CONFIGURATION_DETAILS`* " für Aufgabe (n) in `TaskDefinition - '`*`TASK_DEFINITION`*` '`	Probleme mit der Netzwerkkonfiguration können aufgrund einer fehlenden VPC-Konfiguration oder fehlender oder leerer Subnetze auftreten. Vergewissern Sie sich, dass Ihre Netzwerkkonfiguration korrekt ist. Weitere Informationen finden Sie unter Voraussetzungen für den Zugriff auf Container-Images. Weitere Informationen finden Sie unter Amazon ECS-Aufgabendefinitionsparameter im Amazon Elastic Container Service Developer Guide.

Art des Problems	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
	Aufgaben, die gestartet wurden, als Cluster ein Ausschluss-Tag hatten, sind von der Runtime Monitoring ausgeschlossen. Betroffene Aufgaben-IDs: '*TASK_ID*	Wenn Sie das vordefinierte GuardDuty Tag von `GuardDutyManaged` - in - `true` ändern`false`, GuardDuty werden die Laufzeitereignisse für diesen Amazon ECS-Cluster nicht empfangen. `GuardDuty Managed` Aktualisieren Sie das Tag auf `GuardDutyManaged` - `true` und starten Sie dann die Aufgabe erneut.
	Dienste, die bereitgestellt wurden, als Cluster das Ausschluss-Tag hatten, sind von der Runtime Monitoring ausgeschlossen. Betroffene Dienstnamen: " *SERVICE_NAME*	Wenn Dienste mit dem Ausschluss-Tag `GuardDuty Managed` — bereitgestellt GuardDuty werden`false`, erhalten sie keine Laufzeitereignisse für diesen Amazon ECS-Cluster. Aktualisieren Sie das Tag auf `GuardDutyManaged` - `true` und stellen Sie den Service dann erneut bereit.

Art des Problems	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
	Aufgaben, die vor der Aktivierung der automatisierten Agentenkonfiguration gestartet wurden, werden nicht behandelt. Betroffene Aufgaben-IDs: " *TASK_ID*	Wenn der Cluster eine Aufgabe enthält, die vor der Aktivierung der automatisierten Agentenkonfiguration für Amazon ECS gestartet wurde, kann diese Aufgabe nicht geschützt werden. GuardDuty Starten Sie die Aufgabe erneut, damit sie von überwacht wird. GuardDuty
	Dienste, die vor der Aktivierung der automatisierten Agentenkonfiguration bereitgestellt wurden, sind nicht abgedeckt. Betroffene Dienstnamen: " *SERVICE_NAME*	Wenn Services bereitgestellt werden, bevor die automatische Agentenkonfiguration für Amazon ECS aktiviert wurde, GuardDuty werden keine Laufzeitereignisse für ECS-Cluster empfangen.

Art des Problems	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
	Für den Service *SERVICE_NAME* " ist eine neue Bereitstellung erforderlich fix/troubleshoot. Weitere Informationen finden Sie in der Dokumentation, Betroffene Dienstnamen: " *SERVICE_NAME*	Ein Dienst, der vor der Aktivierung von Runtime Monitoring gestartet wurde, wird nicht unterstützt. Sie können den Service entweder neu starten oder den Service mit der `forceNewDeployment` Option aktualisieren, indem Sie die Schritte unter Aktualisieren eines Amazon ECS-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide befolgen. Alternativ können Sie auch die Schritte unter UpdateService der Amazon Elastic Container Service API-Referenz verwenden.
	Aufgaben, die vor der Aktivierung von Runtime Monitoring gestartet wurden, erfordern einen Neustart. Betroffene Aufgaben-IDs: " *TASK_ID_1*	In Amazon ECS sind die Aufgaben unveränderlich. Um das Laufzeitverhalten einer laufenden AWS Fargate Aufgabe zu beurteilen, stellen Sie sicher, dass Runtime Monitoring bereits aktiviert ist, und starten Sie dann die Aufgabe neu, GuardDuty um den Container-Sidecar hinzuzufügen.

Art des Problems	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
Weitere	Unbekanntes Problem, für Aufgaben in `TaskDefinition - ' TASK_DEFINITION '`	Verwenden Sie die folgenden Fragen, um die Ursache des Problems zu ermitteln: • Wurde die Aufgabe gestartet, bevor Sie Runtime Monitoring aktiviert haben? In Amazon ECS sind die Aufgaben unveränderlich. Um das Laufzeitverhalten einer laufenden Fargate-Aufgabe zu beurteilen, stellen Sie sicher, dass Runtime Monitoring bereits aktiviert ist, und starten Sie dann die Aufgabe neu, GuardDuty um den Container-Sidecar hinzuzufügen. • Ist diese Aufgabe Teil einer Servicebereitstellung, die vor der Aktivierung von Runtime Monitoring gestartet wurde? Falls ja, können Sie den Dienst entweder neu starten oder den Dienst aktualisieren, `forceNewDeployment` indem Sie die Schritte unter Dienst aktualisieren ausführen.

Art des Problems	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
		Sie können auch UpdateService oder verwenden AWS CLI. • Wurde die Aufgabe gestartet, nachdem der ECS-Cluster von Runtime Monitoring ausgeschlossen wurde? Wenn Sie das vordefinierte GuardDuty Tag von `GuardDutyManaged - true` auf `GuardDuty Managed - ändern false`, GuardDuty werden die Laufzeitereignisse für den ECS-Cluster nicht empfangen. • Enthält Ihr Service eine Aufgabe im alten Format von `taskArn`? GuardDuty Runtime Monitoring unterstützt nicht die Erfassung von Aufgaben, die das alte Format von haben `taskArn`. Informationen zu Amazon-Ressourcennamen (ARNs) für Amazon ECS-Ressourcen finden Sie unter

Art des Problems	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
		Amazon-Ressourcennamen (ARNs) und IDs.

Laufzeitabdeckung und Problembehandlung für Amazon EKS-Cluster

Nachdem Sie Runtime Monitoring aktiviert und den GuardDuty Security Agent (Add-on) für EKS entweder manuell oder über die automatische Agentenkonfiguration installiert haben, können Sie mit der Bewertung der Abdeckung Ihrer EKS-Cluster beginnen.

Inhalt

- Überprüfen der Abdeckungsstatistiken
- Änderung des Deckungsstatus durch EventBridge Benachrichtigungen
- Behebung von Problemen mit der Amazon EKS-Laufzeitabdeckung

Überprüfen der Abdeckungsstatistiken

Die Abdeckungsstatistiken für die EKS-Cluster, die Ihren eigenen Konten oder Ihren Mitgliedskonten zugeordnet sind, geben den Prozentsatz der fehlerfreien EKS-Cluster an allen EKS-Clustern in der ausgewählten AWS-Region an. Die folgende Gleichung stellt dies wie folgt dar:

(Fehlerfreie clusters/All Cluster) *100

Wählen Sie eine der Zugriffsmethoden, um die Abdeckungsstatistiken für Ihre Konten einzusehen.

Console

- Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
- Wählen Sie im Navigationsbereich Runtime Monitoring aus.
- Wählen Sie die Registerkarte Laufzeitabdeckung von EKS-Clustern.
- Auf der Registerkarte Laufzeitabdeckung von EKS-Clustern können Sie die Abdeckungsstatistiken einsehen, die nach dem Abdeckungsstatus aggregiert sind, der in der Cluster-Listentabelle verfügbar ist.
  - Sie können die Tabelle mit der Cluster-Liste nach den folgenden Spalten filtern:

  - Cluster name
  - Konto-ID
  - Agentenverwaltungs-Typ
  - Abdeckungsstatus
  - Add-on Version
- Wenn einer Ihrer EKS-Cluster den Abdeckungsstatus Fehlerhaft hat, kann die Spalte Problem zusätzliche Informationen über den Grund für den Status Fehlerhaft enthalten.

API/CLI

- Führen Sie die ListCoverage API mit Ihrer eigenen gültigen Detektor-ID, Region und Service-Endpunkt aus. Mit dieser API können Sie die Cluster-Liste filtern und sortieren.
  - Sie können das Beispiel `filter-criteria` ändern mit einer der folgenden Optionen für `CriterionKey`:
    - `ACCOUNT_ID`
    - `CLUSTER_NAME`
    - `RESOURCE_TYPE`
    - `COVERAGE_STATUS`
    - `ADDON_VERSION`
    - `MANAGEMENT_TYPE`
  - Sie können das Beispiel `AttributeName` in `sort-criteria` ändern mit einer der folgenden Optionen:
    - `ACCOUNT_ID`
    - `CLUSTER_NAME`
    - `COVERAGE_STATUS`
    - `ISSUE`
    - `ADDON_VERSION`
    - `UPDATED_AT`
  - Sie können das ändern *`max-results`* (bis zu 50).
  - Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
 "CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- Führen Sie die GetCoverageStatistics API aus, um aggregierte Statistiken zur Abdeckung abzurufen, die `statisticsType` auf dem basieren.
  - Sie können das Beispiel `statisticsType` zu einer der folgenden Optionen ändern:
    - `COUNT_BY_COVERAGE_STATUS` – Stellt Abdeckungsstatistiken für EKS-Cluster dar, aggregiert nach Abdeckungs-Status.
    - `COUNT_BY_RESOURCE_TYPE`— Abdeckungsstatistiken, aggregiert auf der Grundlage des AWS Ressourcentyps in der Liste.
    - Sie können das Beispiel `filter-criteria` im Befehl ändern. Sie können die folgenden Optionen für `CriterionKey` verwenden:
      - `ACCOUNT_ID`
      - `CLUSTER_NAME`
      - `RESOURCE_TYPE`
      - `COVERAGE_STATUS`
      - `ADDON_VERSION`
      - `MANAGEMENT_TYPE`
  - Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Wenn der Abdeckungsstatus Ihres EKS-Clusters Fehlerhaft ist, finden Sie weitere Informationen unter Behebung von Problemen mit der Amazon EKS-Laufzeitabdeckung.

Änderung des Deckungsstatus durch EventBridge Benachrichtigungen

Der Abdeckungsstatus eines EKS-Clusters in Ihrem Konto wird möglicherweise als Fehlerhaft angezeigt. Um zu erkennen, wann der Abdeckungsstatus Fehlerhaft wird, empfehlen wir Ihnen, den Abdeckungsstatus regelmäßig zu überwachen und Fehler zu beheben, falls der Status Fehlerhaft ist. Alternativ können Sie eine EventBridge Amazon-Regel erstellen, die Sie benachrichtigt, wenn sich der Deckungsstatus von `Unhealthy` zu `Healthy` oder nicht ändert. Veröffentlichen Sie GuardDuty dies standardmäßig im EventBridge Bus für Ihr Konto.

Beispiel für ein Benachrichtigungsschema

In einer EventBridge Regel können Sie anhand der vordefinierten Beispielereignisse und Ereignismuster eine Benachrichtigung über den Versorgungsstatus erhalten. Weitere Informationen zum Erstellen einer EventBridge Regel finden Sie unter Regel erstellen im EventBridge Amazon-Benutzerhandbuch.

Darüber hinaus können Sie mithilfe des folgenden Beispiel-Benachrichtigungsschemas ein benutzerdefiniertes Ereignismuster erstellen. Achten Sie darauf, die Werte für Ihr Konto zu ersetzen. Um benachrichtigt zu werden, wenn sich der Abdeckungsstatus Ihres Amazon EKS-Clusters von `Healthy` zu ändert`Unhealthy`, `detail-type` sollte der sein*`GuardDuty Runtime Protection Unhealthy`*. Um benachrichtigt zu werden, wenn sich der Abdeckungsstatus von `Unhealthy` zu ändert`Healthy`, ersetzen Sie den Wert von `detail-type` durch*`GuardDuty Runtime Protection Healthy`*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "AWS-Konto ID",
  "time": "event timestamp (string)",
  "region": "AWS-Region",
  "resources": [
       ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "EKS",
```

```
        "eksClusterDetails": {
            "clusterName": "string",
            "availableNodes": "string",
             "desiredNodes": "string",
             "addonVersion": "string"
         }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

Behebung von Problemen mit der Amazon EKS-Laufzeitabdeckung

Wenn der Abdeckungsstatus für Ihren EKS-Cluster lautet`Unhealthy`, können Sie den entsprechenden Fehler entweder in der Spalte Problem in der GuardDuty Konsole oder mithilfe des CoverageResource Datentyps anzeigen.

Wenn Sie mit Einschluss- oder Ausschluss-Tags arbeiten, um Ihre EKS-Cluster selektiv zu überwachen, kann es einige Zeit dauern, bis die Tags synchronisiert sind. Dies kann sich auf den Abdeckungsstatus des zugehörigen EKS-Clusters auswirken. Sie können erneut versuchen, das entsprechende Tag (Einschluss oder Ausschluss) zu entfernen und hinzuzufügen. Weitere Informationen finden Sie unter Markieren Ihrer Amazon-EKS-Ressourcen im Amazon-EKS-Entwicklerhandbuch.

Die Struktur eines Abdeckungsproblems ist `Issue type:Extra information`. In der Regel verfügen die Probleme über optionale Zusatzinformationen, die eine spezifische Ausnahme oder eine Beschreibung des Problems enthalten können. Basierend auf zusätzlichen Informationen enthalten die folgenden Tabellen die empfohlenen Schritte zur Behebung der Abdeckungsprobleme für Ihre EKS-Cluster.

Art des Problems (Präfix)	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
Die Erstellung des Addons ist fehlgeschlagen	Das Addon `aws-guard duty-agent` ist nicht mit der aktuellen Cluster-V ersion des Clusters kompatibe l. *`ClusterName`* Das	Stellen Sie sicher, dass Sie eine der Kubernetes-Versionen verwenden, die die Bereitstellung des `aws-guard duty-agent` -EKS-Add-

Art des Problems (Präfix)	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
	angegebene Add-On wird nicht unterstützt.	Ons unterstützen. Weitere Informationen finden Sie unter Kubernetes-Versionen, die vom Security Agent unterstützt werden GuardDuty. Informationen zur Aktualisierung Ihrer Kubernetes-Version finden Sie unter Aktualisieren einer Amazon-EKS-Cluster-Kubernetes-Version.
Die Erstellung des Addons ist fehlgeschlagen Das Addon-Update ist fehlgeschlagen Addon-Status: Ungesund	Problem mit dem EKS-Add-On – `AddonIssueCode` : `AddonIssueMessage`	Informationen zu empfohlenen Schritten für einen bestimmten Add-On-Problemcode finden Sie unter. Troubleshooting steps for Addon creation/ update error with Addon issue code Eine Liste der Addon-Problemcodes, die bei diesem Problem auftreten könnten, finden Sie unter AddonIssue.

Art des Problems (Präfix)	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
Die Erstellung des VPC-Endpoints ist fehlgeschlagen	Die Erstellung von VPC-Endpunkten wird für gemeinsam genutzte VPC nicht unterstützt *vpcId*	Runtime Monitoring unterstützt jetzt die Verwendung einer gemeinsam genutzten VPC innerhalb einer Organisation. Stellen Sie sicher, dass Ihre Konten alle Voraussetzungen erfüllen. Weitere Informationen finden Sie unter Voraussetzungen für die Verwendung einer gemeinsam genutzten VPC.
	Nur wenn Sie eine gemeinsam genutzte VPC mit automatisierter Agentenkonfiguration verwenden Für die Inhaber-Konto-ID *111122223333* für eine gemeinsam genutzte VPC *vpcId* ist weder die Laufzeitüberwachung noch die automatische Agentenkonfiguration oder beides aktiviert.	Das gemeinsame VPC-Besitzerkonto muss Runtime Monitoring und automatische Agentenkonfiguration für mindestens einen Ressourcentyp (Amazon EKS oder Amazon ECS (AWS Fargate)) aktivieren. Weitere Informationen finden Sie unter Spezifische Voraussetzungen für Runtime Monitoring GuardDuty.

Art des Problems (Präfix)	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
	Für die Aktivierung von privatem DNS müssen beide `enableDnsSupport` `enableDnsHostnames` VPC-Attribute auf `true` for *`vpcId`* (Service: Ec2, Status Code:400, Request-ID:) gesetzt sein. *`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`*	Sie müssen jedoch sicherstellen, dass die folgenden VPC-Attribute auf `true` festgelegt sind: `enableDnsSupport` und `enableDnsHostnames` . Weitere Informationen finden Sie unter DNS-Attribute in Ihrer VPC. Wenn Sie Amazon VPC Console unter verwenden, um die Amazon VPC https://console.aws.amazon.com/vpc/ zu erstellen, stellen Sie sicher, dass Sie sowohl DNS-Hostnamen aktivieren als auch DNS-Auflösung aktivieren auswählen. Weitere Informationen finden Sie unter VPC-Konfigurationsoptionen.

Art des Problems (Präfix)	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
Das Löschen des gemeinsamen VPC-Endpoints ist fehlgeschlagen	Das Löschen eines gemeinsamen VPC-Endpunkts für Konto-ID*111122223333* , gemeinsame VPC *vpcId* und Besitzerkonto-ID ist nicht zulässig. *555555555555*	Mögliche Schritte: • Die Deaktivierung des Runtime Monitoring-Status des gemeinsam genutzten VPC-Teilnehmerkontos hat keine Auswirkungen auf die gemeinsame VPC-Endpunktrichtlinie und die Sicherheitsgruppe, die im Besitzerkonto vorhanden ist. Um den gemeinsam genutzten VPC-Endpoint und die Sicherheitsgruppe zu löschen, müssen Sie Runtime Monitoring oder den automatisierten Agent-Konfigurationsstatus im gemeinsam genutzten VPC-Besitzerkonto deaktivieren. • Das gemeinsame VPC-Teilnehmerkonto kann den gemeinsam genutzten VPC-Endpunkt und die Sicherheitsgruppe, die im gemeinsamen VPC-Besitzerkonto gehostet werden, nicht löschen.

Art des Problems (Präfix)	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
Lokale EKS-Cluster	EKS-Add-Ons werden auf lokalen Outpost-Clustern nicht unterstützt.	Nicht umsetzbar. Weitere Informationen finden Sie unter Amazon EKS über Außenposten. AWS
Die Aktivierungsberechtigung für die EKS-Laufzeit-Überwachung wurde nicht erteilt	(kann zusätzliche Informationen anzeigen oder auch nicht)	1. Wenn die zusätzlichen Informationen für dieses Problem verfügbar sind, beheben Sie die Ursache und folgen Sie dem nächsten Schritt. 2. Schalten Sie die EKS-Laufzeit-Überwachung aus und dann wieder ein. Stellen Sie sicher, dass der GuardDuty Agent ebenfalls eingesetzt wird, entweder automatisch GuardDuty oder manuell.
Die Bereitstellung der Ressourcen zur Aktivierung der EKS-Laufzeit-Überwachung wird ausgeführt	(möglicherweise werden zusätzliche Informationen angezeigt)	Nicht umsetzbar. Nachdem Sie die EKS-Laufzeit-Überwachung aktiviert haben, kann der Abdeckungsstatus `Unhealthy` bleiben, bis der Schritt der Ressourcenbereitstellung abgeschlossen ist. Der Abdeckungsstatus wird regelmäßig überwacht und aktualisiert.

Art des Problems (Präfix)	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
Andere (jedes andere Problem)	Fehler aufgrund eines Fehlers bei der Autorisierung	Schalten Sie die EKS-Laufzeit-Überwachung aus und dann wieder ein. Stellen Sie sicher, dass der GuardDuty Agent ebenfalls bereitgestellt wird, entweder automatisch GuardDuty oder manuell.

Schritte zur Fehlerbehebung bei einem creation/update Addon-Fehler mit dem Addon-Problemcode

Fehler beim Erstellen oder Aktualisieren des Addons	Fehlerbehebungsschritte
EKS-Addon-Problem —`InsufficientNumberOfReplicas` : Das Add-on ist fehlerhaft, da es nicht die gewünschte Anzahl an Replikaten hat.	• Anhand der Problemmeldung können Sie die Ursache identifizieren und beheben. Sie können damit beginnen, Ihren Cluster zu beschreiben. Verwenden Sie es beispielsweise, `kubectl describe pods` um die Ursache für den Pod-Ausfall zu identifizieren. Nachdem Sie die Ursache behoben haben, wiederholen Sie den Schritt (Erstellung oder Aktualisierung des Add-Ons). • Wenn das Problem weiterhin besteht, überprüfen Sie, ob der VPC-Endpunkt für Ihren Amazon EKS-Cluster korrekt konfiguriert ist. Weitere Informationen finden Sie unter Validierung der VPC-Endpunktkonfiguration.
EKS-Addon-Problem —`InsufficientNumberOfReplicas` : Das Add-on ist fehlerhaft, weil ein oder mehrere Pods nicht	Um dieses Problem zu beheben, können Sie eine der folgenden Aktionen ausführen:

Fehler beim Erstellen oder Aktualisieren des Addons	Fehlerbehebungsschritte
geplant sind. `0/x` Knoten sind verfügbar:. `x Insufficient cpu. preemption: not eligible due to preemptionPolicy=Never`	• Aktualisieren Sie die Pod-Priorität des GuardDuty Agenten: Konfigurierbare Parameter und Werte indem Sie den `PriorityClass` auf eine der Optionen setzen, die den `preemptionPolicy` Wert als unterstützen. `PreemptLowerPriority` Informationen zur Pod-Priorität finden Sie in der Kubernetes-Dokumentation unter Pod-Priorität und Präemption. • Skalieren Sie die Instance: Informationen zur Verwaltung Ihrer Ressourcen und zur optimalen Instance-Auswahl finden Sie unter Verwalten von Rechenressourcen mithilfe von Knoten und Wählen Sie einen optimalen Amazon EC2-Node-Instance-Typ im Amazon EKS-Benutzerhandbuch. **Note** Die Meldung wird angezeigt`0/x`, weil GuardDuty nur der erste gefundene Fehler gemeldet wird. Die tatsächliche Anzahl der laufenden Pods im GuardDuty Daemonset kann größer als 0 sein.
EKS-Addon-Problem -`InsufficientNumberOfReplicas` : Das Add-on ist fehlerhaft, weil ein oder mehrere Pods nicht geplant sind. `0/x` Knoten sind verfügbar:. `x Too many pods. preemption: not eligible due to preemptionPolicy=Never`	
EKS-Addon-Problem -`InsufficientNumberOfReplicas` : Das Add-on ist fehlerhaft, weil ein oder mehrere Pods nicht geplant sind. `0/x` Knoten sind verfügbar:. `1 Insufficient memory. preemption: not eligible due to preemptionPolicy=Never`	

Fehler beim Erstellen oder Aktualisieren des Addons	Fehlerbehebungsschritte
EKS-Addon-Problem —`InsufficientNumberOfReplicas` : Das Add-on ist fehlerhaft, weil auf einem oder mehreren Pods Container warten `CrashLoopBackOff: Completed`	Sie können die mit dem Pod verknüpften Protokolle einsehen und das Problem identifizieren. Informationen dazu finden Sie unter Debuggen laufender Pods in der Kubernetes-Dokumentation. Verwenden Sie die folgende Checkliste, um dieses Add-On-Problem zu beheben: • Vergewissern Sie sich, dass Runtime Monitoring aktiviert ist. • Stellen Sie sicher, dass dieVoraussetzungen für die Unterstützung von Amazon EKS-Clustern, wie z. B. verifizierte Betriebssystemverteilungen und unterstützte Kubernetes-Versionen, erfüllt sind. • Wenn Sie den Security Agent manuell verwalten, stellen Sie sicher, dass Sie einen VPC-Endpunkt für alle VPCs erstellt haben. Wenn Sie die GuardDuty automatische Konfiguration aktivieren, sollten Sie trotzdem überprüfen, ob der VPC-Endpoint erstellt wird. Zum Beispiel, wenn Sie eine gemeinsam genutzte VPC in einer automatisierten Konfiguration verwenden. Informationen zur Überprüfung finden Sie unterValidierung der VPC-Endpunktkonfiguration. • Vergewissern Sie sich, dass der GuardDuty Security Agent das private DNS des GuardDuty VPC-Endpunkts auflösen kann.

Fehler beim Erstellen oder Aktualisieren des Addons	Fehlerbehebungsschritte
	Informationen zu den Endpunkten finden Sie unter Private DNS-Namen für Endpunkte in. Verwaltung der GuardDuty Sicherheitsagenten Dazu können Sie entweder `nslookup` das Tool unter Windows oder Mac oder das `dig` Tool unter Linux verwenden. Wenn Sie nslookup verwenden, können Sie den folgenden Befehl verwenden, nachdem Sie die Region durch Ihre Region *`us-west-2`* ersetzt haben: `nslookup guardduty-data.` *`us-west-2`* `.amazonaws.com` • Stellen Sie sicher, dass Ihre GuardDuty VPC-Endpunktrichtlinie oder die Service Control-Richtlinie keine Auswirkungen auf die Aktion hat. `guardduty:SendSecurityTelemetry`

Fehler beim Erstellen oder Aktualisieren des Addons	Fehlerbehebungsschritte
EKS-Addon-Problem —`InsufficientNumberOfReplicas` : Das Add-on ist fehlerhaft, weil auf einem oder mehreren Pods Container warten `CrashLoopBackOff: Error`	Sie können die mit dem Pod verknüpften Protokolle einsehen und das Problem identifizieren. Informationen dazu finden Sie unter Debuggen laufender Pods in der Kubernetes-Dokumentation. Nachdem Sie das Problem identifiziert haben, verwenden Sie die folgende Checkliste, um das Problem zu beheben: • Vergewissern Sie sich, dass Runtime Monitoring aktiviert ist. • Stellen Sie sicher, dass dieVoraussetzungen für die Unterstützung von Amazon EKS-Clustern, wie z. B. verifizierte Betriebssystemvereilungen und unterstützte Kubernetes-Versionen, erfüllt sind. • Der GuardDuty Security Agent ist in der Lage, das private DNS des GuardDuty VPC-Endpunkts aufzulösen. Informationen zu den Endpunkten finden Sie unter Private DNS-Namen für Endpunkte in. Verwaltung der GuardDuty Sicherheitsagenten
EKS-Addon-Problem -`AdmissionRequestDenied` : Der Zugangswebhook hat die Anfrage `"validate.kyverno.svc-fail"` abgelehnt: Richtlinie `DaemonSet/amazon-guardduty/aws-guardduty-agent` für Ressourcenverstöße: restrict-image-registries::... `autogen-validate-registries`	1. Der Amazon EKS-Cluster oder der Sicherheitsadministrator müssen die Sicherheitsrichtlinie überprüfen, die das Addon-Update blockiert. 2. Sie müssen entweder den Controller (webhook) deaktivieren oder den Controller die Anfragen von Amazon EKS akzeptieren lassen.

Fehler beim Erstellen oder Aktualisieren des Addons	Fehlerbehebungsschritte
EKS-Addon-Problem —`ConfigurationConflict` : Beim Versuch, sich zu bewerben, wurden Konflikte festgestellt. Wird aufgrund des Konfliktlösungsmodus nicht fortgesetzt. `Conflicts: DaemonSet.apps aws-guardduty-agent - .spec.template.spec.containers[name="aws-guardduty-agent"].image`	Wenn Sie das Addon erstellen oder aktualisieren, geben Sie das `OVERWRITE` Konfliktlösungs-Flag an. Dadurch werden möglicherweise alle Änderungen überschrieben, die mithilfe der Kubernetes-API direkt an den zugehörigen Ressourcen in Kubernetes vorgenommen wurden. Sie können zuerst ein Amazon EKS-Add-on aus einem Cluster entfernen und dann erneut installieren.

Fehler beim Erstellen oder Aktualisieren des Addons	Fehlerbehebungsschritte

EKS-Addon-Problem - `AccessDenied: priorityclasses.scheduling.k8s.io "aws-guardduty-agent.priorityclass" is forbidden: User "eks:addon-manager" cannot patch resource "priorityclasses" in API group "scheduling.k8s.io" at the cluster scope`	Sie müssen die fehlende Berechtigung `eks:addon-cluster-admin ClusterRoleBinding` manuell hinzufügen. Fügen Sie Folgendes `yaml` hinzu`eks:addon-cluster-admin` :
	`---`
	`kind: ClusterRoleBinding`
	`apiVersion: rbac.authorization.k8s.io/v1`
	`metadata:`
	`  name: eks:addon-cluster-admin`
	`subjects:`
	`- kind: User`
	`  name: eks:addon-manager`
	`  apiGroup: rbac.authorization.k8s.io`
	`roleRef:`
	`  kind: ClusterRole`
	`  name: cluster-admin`
	`  apiGroup: rbac.authorization.k8s.io`
	`---`
	Sie können dies jetzt mit `yaml` dem folgenden Befehl auf Ihren Amazon EKS-Cluster anwenden:
	`kubectl apply -f eks-addon-cluster-admin.yaml`

AddonUpdationFailed: EKSAddonIssue - `AccessDenied: namespaces\"amazon-guardduty\"isforbidden:User\"eks:addon-manager\"cannotpatchresource\"namespaces\"inAPIgroup\"\"inthenamespace\"amazon-guardduty\"`	

Fehler beim Erstellen oder Aktualisieren des Addons	Fehlerbehebungsschritte
EKS-Addon-Problem - `AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [all-namespace-must-have-label-owner] All namespaces must have an `owner` label`	Sie müssen entweder den Controller deaktivieren oder dafür sorgen, dass der Controller die Anfragen vom Amazon EKS-Cluster akzeptiert. Bevor Sie das Add-on erstellen oder aktualisieren, können Sie auch einen GuardDuty Namespace erstellen und ihn als `owner` kennzeichnen.
EKS-Addon-Problem - `AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [allowed-container-registries] container <aws-guardduty-agent> has an invalid image registry`	Fügen Sie die Image-Registrierung für GuardDuty `allowed-container-registries` in Ihrem Admission Controller hinzu. Weitere Informationen finden Sie im ECR-Repository für EKS v1.8.1-eks-build.2 in. Amazon ECR-Repository-Hosting-Agent GuardDuty

Einrichten der CPU- und Arbeitsspeicherüberwachung

Nachdem Sie Runtime Monitoring aktiviert und festgestellt haben, dass der Abdeckungsstatus Ihres Clusters fehlerfrei ist, können Sie die Insight-Metriken einrichten und anzeigen.

Anhand der folgenden Themen können Sie beurteilen, wie der bereitgestellte Agent im Vergleich zu den CPU- und Speichergrenzwerten für den GuardDuty Agenten abschneidet.

Überwachung auf dem Amazon ECS-Cluster einrichten

Anhand der folgenden Schritte aus dem CloudWatch Amazon-Benutzerhandbuch können Sie beurteilen, wie der bereitgestellte Agent im Vergleich zu den CPU- und Speicherbeschränkungen für den GuardDuty Agenten abschneidet:

1. Einrichtung von Container Insights auf Amazon ECS für Cluster- und Service-Level-Metriken
2. Amazon ECS Container Insights-Metriken

Überwachung auf dem Amazon EKS-Cluster einrichten

Nachdem der GuardDuty Security Agent bereitgestellt wurde und Sie festgestellt haben, dass der Abdeckungsstatus Ihres Clusters fehlerfrei ist, können Sie die Container Insights-Metriken einrichten und anzeigen.

Bewerten Sie die Leistung des Security Agents

1. Einrichtung von Container Insights auf Amazon EKS und Kubernetes im Amazon-Benutzerhandbuch CloudWatch
2. Amazon EKS- und Kubernetes Container Insights-Metriken im Amazon-Benutzerhandbuch CloudWatch

Managen Sie die Leistung mit dem Security Agent v1.5.0 und höher

Bei Security Agent v1.5.0 und höher können Sie bestimmte Parameter konfigurieren, wenn die Erkenntnisse darauf hindeuten, dass der zugehörige GuardDuty Agent die zugewiesenen Grenzwerte erreicht. Weitere Informationen finden Sie unter Konfigurieren Sie EKS-Add-On-Parameter.

Verwenden von gemeinsam genutzter VPC mit Runtime Monitoring

GuardDuty Runtime Monitoring unterstützt die gemeinsame Nutzung der Amazon Virtual Private Cloud (Amazon VPC) für Sie AWS-Konten , die derselben Organisation angehören. AWS Organizations Sie können gemeinsam genutzte VPC auf zwei Arten verwenden:

- Automatische Agentenkonfiguration (empfohlen) — Wenn der Security Agent GuardDuty automatisch verwaltet wird, konfiguriert er auch die Amazon VPC-Endpunktrichtlinie. Diese Richtlinie basiert auf den gemeinsam genutzten VPC-Einstellungen Ihres Unternehmens.

  Sie müssen die automatische Agentenkonfiguration im gemeinsamen VPC-Besitzerkonto und allen teilnehmenden Konten, die sich diese VPC teilen, aktivieren.
- Manuell verwalteter Agent — Wenn Sie den Security Agent mit gemeinsam genutzter VPC manuell verwalten, müssen Sie die VPC-Endpunktrichtlinie aktualisieren, damit die entsprechenden Konten auf die gemeinsam genutzte VPC zugreifen können. Dazu können Sie die im folgenden Abschnitt veröffentlichte Beispielrichtlinie verwenden. Funktionsweise

  Bei manuellen Verwaltungsszenarien, an denen teilnehmende Konten für gemeinsam genutzte VPC beteiligt sind, ist der Deckungsstatus möglicherweise nicht korrekt. Um sicherzustellen, dass

der Schutz- und Abdeckungsstatus Ihrer Ressourcen auf dem neuesten Stand ist, GuardDuty empfiehlt es sich, die automatische Agentenkonfiguration für alle Konten zu aktivieren, die gemeinsam genutzte VPC verwenden.

Topics

- Funktionsweise
- Voraussetzungen für die Verwendung einer gemeinsam genutzten VPC

Funktionsweise

Diejenigen AWS-Konten , die derselben Organisation angehören wie das gemeinsame Amazon VPC-Besitzerkonto, können auch denselben Amazon VPC-Endpunkt gemeinsam nutzen. Jedes der Konten, die dieselbe Amazon VPC gemeinsam nutzen, wird als AWS Teilnehmerkonto der zugehörigen gemeinsamen Amazon VPC bezeichnet.

Das folgende Beispiel zeigt die Standard-VPC-Endpunktrichtlinie für das gemeinsame VPC-Besitzerkonto und das Teilnehmerkonto. Das `aws:PrincipalOrgID` zeigt die Organisations-ID an, die der gemeinsam genutzten VPC-Ressource zugeordnet ist. Die Verwendung dieser Richtlinie ist auf die Teilnehmerkonten beschränkt, die in der Organisation des Eigentümerkontos vorhanden sind.

Example Beispiel für eine gemeinsam genutzte VPC-Endpunktrichtlinie

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Action": "*",
            "Resource": "*",
            "Effect": "Allow",
            "Principal": "*"
        },
        {
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalOrgID": "o-abcdef0123"
                }
            },
            "Action": "*",
```

```
            "Resource": "*",
            "Effect": "Deny",
            "Principal": "*"
        }
    ]
}
```

Mit GuardDuty automatischer Agentenkonfiguration

Wenn das Eigentümerkonto der gemeinsam genutzten VPC die Laufzeitüberwachung und die automatische Agentenkonfiguration für eine der Ressourcen (Amazon EKS oder AWS Fargate (nur Amazon ECS)) aktiviert, kommen alle gemeinsam genutzten VPCs für die automatische Installation des gemeinsamen Amazon VPC-Endpunkts und der zugehörigen Sicherheitsgruppe im gemeinsamen VPC-Besitzerkonto in Frage. GuardDuty ruft die Organisations-ID ab, die der gemeinsam genutzten Amazon VPC zugeordnet ist.

GuardDuty erstellt einen Amazon VPC-Endpunkt, wenn entweder das gemeinsame VPC-Besitzerkonto oder das teilnehmende Konto ihn benötigt. Beispiele für die Notwendigkeit eines Amazon VPC-Endpunkts sind die Aktivierung von Runtime Monitoring GuardDuty, EKS Runtime Monitoring oder das Starten einer neuen Amazon-Aufgabe. ECS-Fargate Wenn diese Konten Runtime Monitoring und automatische Agentenkonfiguration für einen beliebigen Ressourcentyp aktivieren, GuardDuty wird ein Amazon-VPC-Endpunkt erstellt und die Endpunktrichtlinie mit derselben Organisations-ID wie die des gemeinsam genutzten VPC-Inhaberkontos festgelegt. GuardDuty fügt ein `GuardDutyManaged` Tag hinzu und legt es `true` für den Amazon VPC-Endpunkt fest, der erstellt wird. GuardDuty Wenn das gemeinsam genutzte Amazon VPC-Besitzerkonto für keine der Ressourcen die Laufzeitüberwachung oder die automatische Agentenkonfiguration aktiviert hat, GuardDuty wird die Amazon VPC-Endpunktrichtlinie nicht festgelegt. Informationen zur Konfiguration von Runtime Monitoring und zur automatischen Verwaltung des Security Agents im gemeinsamen VPC-Besitzerkonto finden Sie unter. Laufzeitüberwachung aktivieren GuardDuty

Mit einem manuell verwalteten Agenten verwenden

Wenn Sie eine gemeinsam genutzte VPC mit einem manuell verwalteten Agenten verwenden, stellen Sie sicher, dass es keine explizite `Deny` Endpunktrichtlinie gibt, die Konten blockiert, die die gemeinsam genutzte VPC verwenden müssen. Dadurch wird verhindert, dass der Security Agent Telemetriedaten an diese sendet GuardDuty, was zu einem `Unhealthy` Abdeckungsstatus führt. Informationen zum Einrichten der Endpunktrichtlinie finden Sie unterExample shared VPC endpoint policy.

In Szenarien wie fehlenden Berechtigungen für die gemeinsam genutzte VPC ist die Laufzeitabdeckung möglicherweise nicht korrekt. Sie können die Ressourcenabdeckung kontinuierlich überwachen, indem Sie die Schritte für Ihren Ressourcentyp befolgen. Überprüfung der Statistiken zur Laufzeitabdeckung und Behebung von Problemen

Um den kontinuierlichen Runtime Monitoring-Schutz Ihrer Rechenressourcen zu gewährleisten, GuardDuty empfiehlt es sich, die automatische Agentenkonfiguration für das gemeinsam genutzte VPC-Besitzerkonto und alle teilnehmenden Konten für Ihre Ressourcen zu aktivieren.

Voraussetzungen für die Verwendung einer gemeinsam genutzten VPC

Führen Sie im Rahmen der Ersteinrichtung die folgenden Schritte durch AWS-Konto , damit Sie Eigentümer der gemeinsam genutzten VPC werden können:

1. Eine Organisation erstellen — Erstellen Sie eine Organisation, indem Sie die Schritte unter Erstellen und Verwalten einer Organisation im AWS Organizations Benutzerhandbuch befolgen.

   Informationen zum Hinzufügen oder Entfernen von Mitgliedskonten finden Sie unter Verwaltung AWS-Konten in Ihrer Organisation.
2. Eine gemeinsam genutzte VPC-Ressource erstellen — Sie können eine gemeinsam genutzte VPC-Ressource vom Eigentümerkonto aus erstellen. Weitere Informationen finden Sie im Amazon VPC-Benutzerhandbuch unter Teilen Sie Ihre VPC-Subnetze mit anderen Konten.

Spezifische Voraussetzungen für Runtime Monitoring GuardDuty

Die folgende Liste enthält die spezifischen Voraussetzungen für GuardDuty:

- Das Eigentümerkonto der gemeinsam genutzten VPC und das teilnehmende Konto können von verschiedenen Organisationen stammen. GuardDuty Sie müssen jedoch derselben Organisation in AWS Organizations angehören. Dies ist erforderlich GuardDuty , um einen Amazon VPC-Endpunkt und eine Sicherheitsgruppe für die gemeinsam genutzte VPC zu erstellen. Informationen zur Funktionsweise gemeinsam genutzter VPCs finden Sie unter Teilen Sie Ihre VPC mit anderen Konten im Amazon VPC-Benutzerhandbuch.
- Aktivieren Sie Runtime Monitoring oder EKS Runtime Monitoring sowie die GuardDuty automatische Agentenkonfiguration für alle Ressourcen im gemeinsamen VPC-Besitzerkonto und im Teilnehmerkonto. Weitere Informationen finden Sie unter Laufzeitüberwachung aktivieren.

Wenn Sie diese Konfigurationen bereits abgeschlossen haben, fahren Sie mit dem nächsten Schritt fort.

- Wenn Sie entweder mit einer Amazon EKS- oder einer Amazon ECS-Aufgabe (AWS Fargate nur) arbeiten, stellen Sie sicher, dass Sie die gemeinsam genutzte VPC-Ressource auswählen, die dem Eigentümerkonto zugeordnet ist, und wählen Sie deren Subnetze aus.

Verwendung von Infrastructure as Code (IaC) mit GuardDuty automatisierten Sicherheitsagenten

Verwenden Sie diesen Abschnitt nur, wenn die folgende Liste auf Ihren Anwendungsfall zutrifft:

- Sie verwenden Infrastructure as Code (IaC) -Tools wie AWS Cloud Development Kit (AWS CDK) und Terraform, um Ihre AWS Ressourcen zu verwalten, und
- Sie müssen die GuardDuty automatische Agentenkonfiguration für einen oder mehrere Ressourcentypen aktivieren — Amazon EKS, Amazon EC2 oder Amazon. ECS-Fargate

Überblick über das Diagramm zur Abhängigkeit von IaC-Ressourcen

Wenn Sie die GuardDuty automatische Agentenkonfiguration für einen Ressourcentyp aktivieren, erstellt GuardDuty automatisch einen VPC-Endpunkt und eine Sicherheitsgruppe, die diesem VPC-Endpunkt zugeordnet ist, und installiert den Security Agent für diesen Ressourcentyp. Standardmäßig GuardDuty werden der VPC-Endpunkt und die zugehörige Sicherheitsgruppe erst gelöscht, nachdem Sie Runtime Monitoring deaktiviert haben. Weitere Informationen finden Sie unter Deaktivieren, Deinstallieren und Bereinigen von Ressourcen in Runtime Monitoring.

Wenn Sie ein IaC-Tool verwenden, verwaltet es ein Abhängigkeitsdiagramm der Ressourcen. Beim Löschen von Ressourcen mithilfe des IaC-Tools werden nur Ressourcen gelöscht, die als Teil des Abhängigkeitsdiagramms der Ressourcen nachverfolgt werden können. IaC-Tools wissen möglicherweise nichts über die Ressourcen, die außerhalb ihrer angegebenen Konfiguration erstellt wurden. Sie erstellen beispielsweise eine VPC mit einem IaC-Tool und fügen dieser VPC dann mithilfe einer AWS Konsole oder eines API-Vorgangs eine Sicherheitsgruppe hinzu. Im Diagramm zur Ressourcenabhängigkeit hängt die VPC-Ressource, die Sie erstellen, von der zugehörigen Sicherheitsgruppe ab. Wenn Sie diese VPC-Ressource mithilfe des IaC-Tools löschen, erhalten Sie eine Fehlermeldung. Sie können diesen Fehler umgehen, indem Sie die zugehörige

Sicherheitsgruppe manuell löschen oder die IaC-Konfiguration so aktualisieren, dass sie diese hinzugefügte Ressource einschließt.

Häufiges Problem — Löschen von Ressourcen in IaC

Wenn Sie die GuardDuty automatische Agentenkonfiguration verwenden, möchten Sie möglicherweise eine Ressource (Amazon EKS, Amazon EC2 oder Amazon ECS-Fargate) löschen, die Sie mit einem IAC-Tool erstellt haben. Diese Ressource ist jedoch von einem VPC-Endpunkt abhängig, der erstellt wurde. GuardDuty Dadurch wird verhindert, dass das IaC-Tool die Ressource selbst löscht, und Sie müssen die Laufzeitüberwachung deaktivieren, wodurch der VPC-Endpunkt automatisch gelöscht wird.

Wenn Sie beispielsweise versuchen, den VPC-Endpunkt zu löschen, der in Ihrem Namen GuardDuty erstellt wurde, erhalten Sie eine Fehlermeldung, die den folgenden Beispielen ähnelt.

Example

Beispiel für einen Fehler bei der Verwendung von CDK

```
The following resource(s) failed to delete:
 [mycdkvpcapplicationpublicsubnet1Subnet1SubnetEXAMPLE1, mycdkvpcapplicationprivatesubnet1Subne
Resource handler returned message: "The subnet 'subnet-APKAEIVFHP46CEXAMPLE' has
 dependencies and cannot be deleted. (Service: Ec2, Status Code: 400, Request
 ID: e071c3c5-7442-4489-838c-0dfc6EXAMPLE)" (RequestToken: 4381cff8-6240-208a-8357-5557b7EXAMPL
 HandlerErrorCode: InvalidRequest)
```

Example

Fehlerbeispiel bei der Verwendung von Terraform

```
module.vpc.aws_subnet.private[1]: Still destroying... [id=subnet-APKAEIVFHP46CEXAMPLE,
 19m50s elapsed]
module.vpc.aws_subnet.private[1]: Still destroying... [id=subnet-APKAEIVFHP46CEXAMPLE,
 20m0s elapsed]

Error: deleting EC2 Subnet (subnet-APKAEIBAERJR2EXAMPLE): DependencyViolation: The
 subnet 'subnet-APKAEIBAERJR2EXAMPLE' has dependencies and cannot be deleted.
       status code: 400, request id: e071c3c5-7442-4489-838c-0dfc6EXAMPLE
```

> **Note**
>
> Die AWS Terraform-Anbieter-Version 6.43.0 und höher behebt dieses Problem automatisch. Der AWS Anbieter erkennt und entfernt währenddessen GuardDuty-managed VPC-Endpunkte und Sicherheitsgruppen. `terraform destroy` Dieser Fix gilt für alle Ressourcentypen (Amazon EKS, Amazon EC2 und Amazon). ECS-Fargate

Lösung — Problem mit dem Löschen von Ressourcen verhindern

In diesem Abschnitt können Sie den VPC-Endpunkt und die Sicherheitsgruppe unabhängig von GuardDuty verwalten.

Führen Sie die folgenden Schritte in der angegebenen Reihenfolge aus, um das vollständige Eigentum an den Ressourcen zu erlangen, die mit dem IaC-Tool konfiguriert wurden:

1. Erstellen Sie eine VPC. Um Zugriffsberechtigungen zu gewähren, ordnen Sie dieser GuardDuty VPC einen VPC-Endpunkt der Sicherheitsgruppe zu.
2. Aktivieren Sie die GuardDuty automatische Agentenkonfiguration für Ihren Ressourcentyp

Nachdem Sie die vorherigen Schritte abgeschlossen haben, erstellt GuardDuty das Unternehmen keinen eigenen VPC-Endpunkt und verwendet den, den Sie mit dem IaC-Tool erstellt haben, wieder.

Informationen zum Erstellen Ihrer eigenen VPC finden Sie unter Erstellen Sie eine VPC nur in den Amazon VPC Transit Gateways. Informationen zum Erstellen eines VPC-Endpunkts finden Sie im folgenden Abschnitt für Ihren Ressourcentyp:

- Informationen zu Amazon EC2 finden Sie unter. Voraussetzung — Manuelles Erstellen des Amazon VPC-Endpunkts
- Informationen zu Amazon EKS finden Sie unterVoraussetzung — Erstellen eines Amazon VPC-Endpunkts.

Gesammelte Runtime-Ereignistypen, die GuardDuty verwendet

Der GuardDuty Security Agent sammelt die folgenden Ereignistypen und sendet sie zur Erkennung und Analyse von Bedrohungen an das GuardDuty Backend. GuardDuty macht diese Ereignisse für Sie nicht zugänglich. Wenn eine potenzielle Bedrohung GuardDuty erkannt und eine generiert

wirdBei der Laufzeitüberwachung werden Typen gefunden, können Sie sich die entsprechenden Befunddetails ansehen.

Informationen zur GuardDuty Verwendung der gesammelten Ereignistypen in Runtime Monitoring finden Sie unterAbmeldung von der Verwendung Ihrer Daten zur Serviceverbesserung.

Ereignisse verarbeiten

Prozessereignisse stellen Informationen dar, die mit den Prozessen verknüpft sind, die auf Amazon EC2-Instances und Container-Workloads ausgeführt werden. Die folgende Tabelle enthält die Feldnamen und Beschreibungen der Prozessereignisse, die Runtime Monitoring erfasst, um potenzielle Bedrohungen zu erkennen.

Feldname	Description
Prozessname	Name des beobachteten Prozesses.
Prozesspfad	Absoluter Pfad der ausführbaren Datei des Prozesses.
Prozess-ID	Die ID, die dem Prozess vom Betriebssystem zugewiesen wurde.
Namespace-PID	Die Prozess-ID des Prozesses in einem sekundären PID-Namespace, bei dem es sich nicht um den PID-Namespace auf Host-Ebene handelt. Bei Prozessen innerhalb eines Containers ist dies die Prozess-ID, die innerhalb des Containers beobachtet wird.
Prozess-Benutzer-ID	Die eindeutige ID des Benutzers, der den Prozess ausgeführt hat.
Prozess-UUID	Die eindeutige ID, die dem Prozess von zugewiesen wurde GuardDuty.
Prozess-GID	Prozess-ID der Prozessgruppe.
Prozess-EGID	Effektive Gruppen-ID der Prozessgruppe.

Feldname	Description
Prozess-EUID	Effektive Benutzer-ID des Prozesses.
Prozess-Benutzername	Der Benutzername, der den Prozess ausgeführt hat.
Prozesses-Startzeit	Die Zeit, zu der der Prozess erstellt wurde. Dieses Feld hat das UTC-Datums-Zeichenfolgenformat (`2023-03-22T19:37:20.168Z`).
Ausführbarer Prozess SHA-256	Der Hash `SHA256` der ausführbaren Prozessesdatei.
Prozess-Skriptpfad	Pfad der Skriptdatei, die ausgeführt wurde.
Prozess-Umgebungsvariable	Die Umgebungsvariable, die dem Prozess zur Verfügung gestellt wurde. Nur `LD_PRELOAD` und `LD_LIBRARY_PATH` werden gesammelt.
Aktuelles Arbeitsverzeichnis (PWD) des Prozesses	Derzeitiges Arbeitsverzeichnis des Prozesses.
Übergeordneter Prozess	Prozessdetails des übergeordneten Prozesses. Ein übergeordneter Prozess ist ein Prozess, der den beobachteten Prozess erzeugt hat.

Feldname	Description
Befehlszeilen-Argumente Derzeit ist dieses Feld auf bestimmte Agentenversionen beschränkt, die dem Ressourcentyp entsprechen: • Fargate (nur Amazon ECS) mit GuardDuty Security Agent v1.0.0 und höher. • Amazon EC2-Instances mit GuardDuty Security Agent v1.0.0 und höher. • Amazon EKS-Cluster mit Security Agent v1.4.0 und höher. Weitere Informationen finden Sie unter GuardDuty Release-Versionen des Security Agents.	Command-line Argumente, die zum Zeitpunkt der Prozessausführung bereitgestellt werden. Dieses Feld kann vertrauliche Kundendaten enthalten.

Container-Ereignisse

Container-Ereignisse stellen Informationen dar, die mit den Aktivitäten der Container-Workloads verknüpft sind. Die folgende Tabelle enthält die Feldnamen und Beschreibungen der Container-Workload-Ereignisse, die Runtime Monitoring erfasst, um potenzielle Bedrohungen zu erkennen.

Feldname	Description
Container-Name	Name des Containers. Falls verfügbar, zeigt dieses Feld den Wert des Labels `io.kubenetes.container.name` an.
Container-UID	Die eindeutige ID des Containers, die von der Container-Laufzeit zugewiesen wurde.
Container-Laufzeit	Die Container-Laufzeit (wie z. B. `docker` oder `containerd`), die zum Ausführen des Containers verwendet wurde.

Feldname	Description
Container-Image-ID	Die ID des Container-Images.
Container-Image-Name	Name des Container-Images.

AWS Fargate Aufgabenereignisse (nur Amazon ECS)

Fargate-Amazon ECS-Aufgabenereignisse stellen Aktivitäten im Zusammenhang mit Amazon ECS-Aufgaben dar, die auf Fargate-Computern ausgeführt werden. Die folgende Tabelle enthält die Feldnamen und Beschreibungen der ECS-Fargate Amazon-Aufgabenereignisse, die Runtime Monitoring erfasst, um potenzielle Bedrohungen zu erkennen.

Feldname	Description
Amazon-Ressourcenname (ARN) der Aufgabe	Der ARN der Aufgabe.
Cluster-Name	Der Name des Amazon ECS-Clusters.
Familienname	Der Familienname der Aufgabendefinition. Der `family` wird als Name für die Aufgabendefinition verwendet, die zum Starten der Aufgabe verwendet wird.
Service-Name	Der Name des Amazon ECS-Service, wenn die Aufgabe als Teil eines Dienstes gestartet wurde.
Starttyp	Die Infrastruktur, auf der Ihre Aufgabe ausgeführt wird. Für Runtime Monitoring mit dem Ressourcentyp als `ECSCluster` könnte der Starttyp entweder `EC2` oder sein`FARGATE`.
CPU	Die Anzahl der CPU-Einheiten, die von der Aufgabe verwendet werden, wie in der Aufgabendefinition ausgedrückt.

Kubernetes-Pod-Ereignisse

Die folgende Tabelle enthält die Feldnamen und Beschreibungen der Kubernetes-Pod-Ereignisse, die Runtime Monitoring erfasst, um potenzielle Bedrohungen zu erkennen.

Feldname	Description
Pod-ID	Die ID des Kubernetes-Pods.
Pod-Name	Name des Kubernetes-Pods.
Pod-Namespace	Name des Kubernetes-Namespace, zu dem der Kubernetes-Workload gehört.
Kubernetes-Cluster-Name	Name des Kubernetes-Clusters.

DNS-Ereignisse (Domain Name System)

Die DNS-Ereignisse (Domain Name System) enthalten Details zu den DNS-Abfragen, die von Ihren Ressourcentypen gestellt wurden, und die entsprechenden Antworten. Die folgende Tabelle enthält die Feldnamen und Beschreibungen der DNS-Ereignisse, die Runtime Monitoring erfasst, um potenzielle Bedrohungen zu erkennen.

Feldname	Description
Socket-Typ	Socket-Typ zur Angabe der Kommunikationssemantik. Beispiel, `SOCK_RAW`.
Adress-Familie	Stellt das der Adresse zugeordnete Kommunikationsprotokoll dar. Die Adressfamilie `AF_INET` wird beispielsweise für das IPv4-Protokoll verwendet.
Richtungs-ID	Die ID der Verbindungsrichtung.
Protokollnummer	Die Layer-4-Protokollnummer, z. B. 17 für UDP und 6 für TCP.
DNS-Remote-Endpunkt-IP	Die Remote-IP-Informationen der Verbindung.

Feldname	Description
DNS-Remote-Endpunkt-Port	Die Portnummer der Verbindung.
Lokale DNS-Endpunkt-IP	Die lokale IP der Verbindung.
Lokaler DNS-Endpunkt-Port	Die Portnummer der Verbindung.
DNS-Nutzlast	Die Nutzlast von DNS-Paketen, die DNS-Abfragen und -Antworten enthalten.

Offene Ereignisse

Offene Ereignisse sind mit Dateizugriffen und Dateiänderungen verbunden. Die folgende Tabelle enthält die Feldnamen und Beschreibungen der offenen Ereignisse, die Runtime Monitoring erfasst, um potenzielle Bedrohungen zu erkennen.

Feldname	Description
Dateipfad	Pfad der Datei, die in diesem Ereignis geöffnet wird.
Flags	Beschreibt den Dateizugriffsmodus, z. B. Schreibgeschützt, Nur-Schreiben und Lesen-Schreiben.

Lastmodul-Ereignis

Die folgende Tabelle enthält den Feldnamen und die Beschreibung des Lademodul-Ereignisses, das Runtime Monitoring erfasst, um potenzielle Bedrohungen zu erkennen.

Feldname	Description
Modulname	Name des in den Kernel geladenen Moduls.

Mprotect-Ereignisse

Mprotect-Ereignisse liefern Informationen über Änderungen der Speicherschutzeinstellungen der Prozesse, die auf den überwachten Systemen ausgeführt werden. Die folgende Tabelle enthält die Feldnamen und Beschreibungen der Mprotect-Ereignisse, die Runtime Monitoring erfasst, um potenzielle Bedrohungen zu erkennen.

Feldname	Description
Adressbereiche	Der Adressbereich, für den der Zugriffsschutz geändert wurde.
Arbeitsspeicherregionen	Gibt den Bereich des Adressraums eines Prozesses an, z. B. Stack und Heap.
Flags	Stellt Optionen dar, die das Verhalten dieses Ereignisses steuern.

Mount-Ereignisse

Mount-Ereignisse liefern Informationen zum Mounten und Unmounten von Dateisystemen auf Ihrer überwachten Ressource. Die folgende Tabelle enthält die Feldnamen und Beschreibungen der Mount-Ereignisse, die Runtime Monitoring erfasst, um potenzielle Bedrohungen zu erkennen.

Feldname	Description
Mount-Ziel	Der Pfad, in dem die Mount-Quelle gemountet ist.
Mount-Quelle	Der Pfad auf dem Host, der am Mount-Ziel gemountet ist.
Typ des Dateisystems	Repräsentiert den Typ des bereitgestellten Dateisystems.
Flags	Stellt Optionen dar, die das Verhalten dieses Ereignisses steuern.

Verknüpfungs-Ereignisse

Link-Ereignisse bieten einen Überblick über die Link-Management-Aktivitäten im Dateisystem in Ihren überwachten Ressourcen. Die folgende Tabelle enthält die Feldnamen und Beschreibungen der Linkereignisse, die Runtime Monitoring erfasst, um potenzielle Bedrohungen zu erkennen.

Feldname	Description
Verknüpfungs-Pfad	Pfad, in dem der Hardlink erstellt wird.
Zielpfad	Pfad der Datei, auf die der Hardlink verweist.

Symlink-Ereignisse

Symlink-Ereignisse bieten Einblick in die Aktivitäten zur Verwaltung symbolischer Links im Dateisystem in Ihren überwachten Ressourcen. Die folgende Tabelle enthält die Feldnamen und Beschreibungen der Symlink-Ereignisse, die Runtime Monitoring erfasst, um potenzielle Bedrohungen zu erkennen.

Feldname	Description
Verknüpfungs-Pfad	Pfad, in dem der symbolische Link erstellt wird.
Zielpfad	Pfad der Datei, auf die der symbolische Link verweist.

Dup-Ereignisse

Dup-Ereignisse bieten Einblick in die Duplizierung von Dateideskriptoren durch Prozesse, die auf den überwachten Ressourcen ausgeführt werden. Die folgende Tabelle enthält die Feldnamen und Beschreibungen der Dup-Ereignisse, die Runtime Monitoring erfasst, um potenzielle Bedrohungen zu erkennen.

Feldname	Description
Alter Dateideskriptor	Ein Dateideskriptor, der ein geöffnetes Dateiobjekt darstellt.

Feldname	Description
Neuer Dateideskriptor	Ein neuer Dateideskriptor, der ein Duplikat des alten Dateidesk riptors ist. Sowohl der alte als auch der neue Dateideskriptor stehen für dasselbe offene Dateiobjekt.
DNS-Remote-Endpunkt-IP	Die Remote-IP-Adresse des Netzwerk-Sockets, dargestel lt durch den alten Dateideskriptor. Gilt nur, wenn der alte Dateideskriptor einen Netzwerk-Socket darstellt.
DNS-Remote-Endpunkt-Port	Die Remote-IP-Adresse des Netzwerk-Sockets, dargestel lt durch den alten Dateideskriptor. Gilt nur, wenn der alte Dateideskriptor einen Netzwerk-Socket darstellt.
Lokale Dup-Endpunkt-IP	Die lokale IP-Adresse des Netzwerk-Sockets, dargestellt durch den alten Dateideskriptor. Gilt nur, wenn der alte Dateideskriptor einen Netzwerk-Socket darstellt.
Lokaler Dup-Endpunkt-Port	Der lokale Port des Netzwerk-Sockets, dargestellt durch den alten Dateideskriptor. Gilt nur, wenn der alte Dateideskriptor einen Netzwerk-Socket darstellt.

Arbeitsspeicherzuordnungs-Ereignis

Die folgende Tabelle enthält den Feldnamen und die Beschreibung der Speicherzuordnungsereignisse, die Runtime Monitoring erfasst, um potenzielle Bedrohungen zu erkennen.

Feldname	Description
Dateipfad	Pfad der Datei, der der Arbeitsspeicher zugeordnet ist.

Socket-Ereignisse

Socket-Ereignisse liefern Informationen über die Netzwerk-Socket-Verbindungen, die für die Aktivitäten der überwachten Ressourcen verwendet werden. Die folgende Tabelle enthält die

Feldnamen und Beschreibungen der Socket-Ereignisse, die Runtime Monitoring erfasst, um potenzielle Bedrohungen zu erkennen.

Feldname	Description
Adress-Familie	Stellt das der Adresse zugeordnete Kommunikationsprotokoll dar. Die Adressfamilie `AF_INET` wird beispielsweise für das IPv4-Protokoll verwendet.
Socket-Typ	Socket-Typ zur Angabe der Kommunikationssemantik. Beispiel, `SOCK_RAW`.
Protokollnummer	Spezifiziert ein bestimmtes Protokoll innerhalb der Adressfam ilie. Normalerweise gibt es ein einziges Protokoll in Adressfam ilien. Beispielsweise hat die Adressfamilie `AF_INET` nur das IP-Protokoll.

Verbindungs-Ereignisse

Connect-Ereignisse bieten Einblick in die Netzwerkverbindungen, die durch die Prozesse auf Ihren überwachten Ressourcen hergestellt wurden. Die folgende Tabelle enthält die Feldnamen und Beschreibungen der Verbindungsereignisse, die Runtime Monitoring erfasst, um potenzielle Bedrohungen zu erkennen.

Feldname	Description
Adress-Familie	Stellt das der Adresse zugeordnete Kommunikationsprotokoll dar. Die Adressfamilie `AF_INET` wird beispielsweise für das IPv4-Protokoll verwendet.
Socket-Typ	Socket-Typ zur Angabe der Kommunikationssemantik. Beispiel, `SOCK_RAW`.
Protokollnummer	Spezifiziert ein bestimmtes Protokoll innerhalb der Adressfam ilie. Normalerweise gibt es ein einziges Protokoll in Adressfam ilien. Beispielsweise hat die Adressfamilie `AF_INET` nur das IP-Protokoll.

Feldname	Description
Dateipfad	Pfad der Socket-Datei, falls die Adressfamilie `AF_UNIX` ist.
Remote-Endpunkt-IP	Die Remote-IP-Informationen der Verbindung.
Remote-Endpunkt-Port	Die Portnummer der Verbindung.
Lokale Endpunkt-IP	Die lokale IP der Verbindung.
Lokaler Endpunkt-Port	Die Portnummer der Verbindung.

Prozess-VM-Readv-Ereignisse

Die Readv-Ereignisse der Prozess-VM bieten Einblick in die Lesevorgänge, die von den Prozessen in ihren eigenen virtuellen Speicherbereichen ausgeführt werden. Die folgende Tabelle enthält die Feldnamen und Beschreibungen der Readv-Ereignisse der Prozess-VM, die Runtime Monitoring erfasst, um potenzielle Bedrohungen zu erkennen.

Feldname	Description
Flags	Stellt Optionen dar, die das Verhalten dieses Ereignisses steuern.
Ziel-PID	Prozess-ID des Prozesses, aus dessen Arbeitsspeicher gelesen wird.
UUID des Zielprozesses	Die eindeutige ID des Zielprozesses.
Pfad der ausführbaren Zieldatei	Absoluter Pfad der ausführbaren Zieldatei des Prozesses.

Prozess-VM-Writev-Ereignisse

Write-Ereignisse der Prozess-VM bieten Einblick in die Schreibvorgänge, die von den Prozessen in ihren eigenen virtuellen Speicherbereichen ausgeführt werden. Die folgende Tabelle enthält die Feldnamen und Beschreibungen der Schreibereignisse der Prozess-VM, die Runtime Monitoring erfasst, um potenzielle Bedrohungen zu erkennen.

Feldname	Description
Flags	Stellt Optionen dar, die das Verhalten dieses Ereignisses steuern.
Ziel-PID	Prozess-ID des Prozesses, in den Arbeitsspeicher geschrieben wird.
UUID des Zielprozesses	Die eindeutige ID des Zielprozesses.
Pfad der ausführbaren Zieldatei	Absoluter Pfad der ausführbaren Zieldatei des Prozesses.

Process Trace (Ptrace) -Ereignisse

Der Systemaufruf Process Trace (Ptrace) ist ein Debugging- und Ablaufverfolgungsmechanismus, der es einem Prozess (Tracer) ermöglicht, die Ausführung eines anderen Prozesses (Tracee) zu beobachten und zu steuern. Dies gibt dem Tracer die Möglichkeit, den Speicher, die Register und den Ausführungsablauf des Zielprozesses zu überprüfen und zu ändern.

Ptrace-Ereignisse bieten Einblick in die Verwendung des Ptrace-Systemaufrufs durch Prozesse, die auf den überwachten Ressourcen ausgeführt werden. Die folgende Tabelle enthält die Feldnamen und Beschreibungen der Ptrace-Ereignisse, die Runtime Monitoring erfasst, um potenzielle Bedrohungen zu erkennen.

Feldname	Description
Ziel-PID	Prozess-ID des Zielprozesses.
UUID des Zielprozesses	Die eindeutige ID des Zielprozesses.
Pfad der ausführbaren Zieldatei	Absoluter Pfad der ausführbaren Zieldatei des Prozesses.
Flags	Stellt Optionen dar, die das Verhalten dieses Ereignisses steuern.

Ereignisse binden

Bind-Ereignisse bieten Einblick in die Bindung von Netzwerk-Sockets durch Prozesse, die auf den überwachten Ressourcen ausgeführt werden. Die folgende Tabelle enthält die Feldnamen und Beschreibungen der Bindereignisse, die Runtime Monitoring erfasst, um potenzielle Bedrohungen zu erkennen.

Feldname	Description
Adress-Familie	Stellt das der Adresse zugeordnete Kommunikationsprotokoll dar. Die Adressfamilie `AF_INET` wird beispielsweise für das IPv4-Protokoll verwendet.
Socket-Typ	Socket-Typ zur Angabe der Kommunikationssemantik. Beispiel, `SOCK_RAW`.
Protokollnummer	Die Layer-4-Protokollnummer, z. B. 17 für UDP und 6 für TCP.
Lokale Endpunkt-IP	Die lokale IP der Verbindung.
Lokaler Endpunkt-Port	Die Portnummer der Verbindung.

Ereignisse anhören

Listen-Ereignisse geben Aufschluss über den Empfangsstatus von Netzwerk-Sockets und geben an, ob ein Netzwerk-Socket bereit ist, eingehende Verbindungen anzunehmen. Ein Prozess, der auf Ihrer überwachten Ressource ausgeführt wird, versetzt den Netzwerk-Socket in einen Listening-Zustand. Die folgende Tabelle enthält die Feldnamen und Beschreibungen der Listen-Ereignisse, die Runtime Monitoring erfasst, um potenzielle Bedrohungen zu erkennen.

Feldname	Description
Adress-Familie	Stellt das der Adresse zugeordnete Kommunikationsprotokoll dar. Die Adressfamilie `AF_INET` wird beispielsweise für das IPv4-Protokoll verwendet.
Socket-Typ	Socket-Typ zur Angabe der Kommunikationssemantik. Beispiel, `SOCK_RAW`.

Feldname	Description
Protokollnummer	Die Layer-4-Protokollnummer, z. B. 17 für UDP und 6 für TCP.
Lokale Endpunkt-IP	Die lokale IP der Verbindung.
Lokaler Endpunkt-Port	Die Portnummer der Verbindung.

Ereignisse umbenennen

Umbenennungsereignisse liefern Informationen über das Umbenennen von Dateien und Verzeichnissen durch Prozesse, die auf den überwachten Ressourcen ausgeführt werden. Die folgende Tabelle enthält die Feldnamen und Beschreibungen der Umbenennungsereignisse, die Runtime Monitoring erfasst, um potenzielle Bedrohungen zu erkennen.

Feldname	Description
Dateipfad	Pfad der Datei, die umbenannt wird.
Target	Der neue Pfad der Datei.

Legen Sie Benutzer-ID-Ereignisse (UID) fest

Set-User-ID (UID) -Ereignisse bieten Einblick in die Änderungen, die an der Benutzer-ID (UID) vorgenommen wurden, die mit den laufenden Prozessen auf Ihren überwachten Ressourcen verknüpft ist. Die folgende Tabelle enthält die Feldnamen und Beschreibungen der festgelegten UID-Ereignisse, die Runtime Monitoring erfasst, um potenzielle Bedrohungen zu erkennen.

Feldname	Description
Neue EUID	Die neue effektive Benutzer-ID des Prozesses.
Neue UID	Die neue Benutzer-ID des Prozesses.

Chmod-Ereignisse

Chmod-Ereignisse bieten Einblick in die Änderungen der Berechtigungen (Modus) von Dateien und Verzeichnissen auf den überwachten Ressourcen. Die folgende Tabelle enthält die Feldnamen und Beschreibungen der chmod-Ereignisse, die Runtime Monitoring erfasst, um potenzielle Bedrohungen zu erkennen.

Feldname	Description
Dateipfad	Pfad der Datei, die dieses Ereignis auslöst.
Dateimodus	Die aktualisierten Zugriffsberechtigungen für die zugehörige Datei.

Amazon ECR-Repository-Hosting-Agent GuardDuty

In den folgenden Abschnitten sind die Amazon Elastic Container Registry (Amazon ECR) -Repositorys aufgeführt, in denen der Sicherheitsagent GuardDuty gehostet wird, der auf Ihren Amazon EKS-, Amazon ECS- und Amazon ECS-Amazon EC2 Bottlerocket-Ressourcen bereitgestellt wird.

Voraussetzung dafür ist, dass Sie Voraussetzungen für den Zugriff auf Container-Images eine Rolle zur Aufgabenausführung angeben, die über bestimmte Amazon Elastic Container Registry (Amazon ECR) -Berechtigungen verfügt. Um diese Berechtigungen weiter einzuschränken, können Sie die Amazon ECR-Repository-URI hinzufügen, die den GuardDuty Agenten für Fargate-Amazon ECS-Ressourcen hostet.

Inhalt

- ECR-Repository für die EKS-Agentenversionen 1.16.0 - 1.8.1 (eks.build.2)
- ECR-Repository für EKS-Agenten Version 1.8.1 (eks.build.1)
- ECR-Repository für Agenten an GuardDuty AWS Fargate (Nur Amazon ECS)
- ECR-Repository für GuardDuty Agenten auf Bottlerocket ECS-EC2

ECR-Repository für die EKS-Agentenversionen 1.16.0 - 1.8.1 (eks.build.2)

Wenn Sie die GuardDuty automatische Konfiguration für Runtime Monitoring for EKS aktivieren, GuardDuty wird diese Agentenversion auf Ihren Amazon EKS-Clustern bereitgestellt. Informationen zur Aktivierung des automatisierten Agenten finden Sie unterAutomatische Verwaltung des Security Agents für Amazon EKS-Ressourcen.

Die folgende Tabelle zeigt die Amazon ECR-Repository-URIs, auf denen die GuardDuty Security Agent-Versionen `1.16.0.eks.build.21.15.0.eks.build.2`,`1.11.0.eks.build.2`, `1.10.0.eks.build.21.9.0.eks.build.2`, und `1.8.0.eks.build.2` für Amazon EKS gehostet werden.

AWS-Region	Amazon-ECR-Repository-URI
USA West (Oregon)	`602401143452.dkr.ecr.us-west-2.amazonaws.com`
	`039403964562.dkr.ecr.us-west-2.amazonaws.com`
Europa (Paris)	`602401143452.dkr.ecr.eu-west-3.amazonaws.com`
	`113643092156.dkr.ecr.eu-west-3.amazonaws.com`
Asien-Pazifik (Mumbai)	`602401143452.dkr.ecr.ap-south-1.amazonaws.com`
	`610108029387.dkr.ecr.ap-south-1.amazonaws.com`
Asien-Pazifik (Hyderabad)	`900889452093.dkr.ecr.ap-south-2.amazonaws.com`
	`618745550137.dkr.ecr.ap-south-2.amazonaws.com`

AWS-Region	Amazon-ECR-Repository-URI
Kanada (Zentral)	602401143452.dkr.ecr.ca-central-1.amazonaws.com
	001188825231.dkr.ecr.ca-central-1.amazonaws.com
Kanada West (Calgary)	761377655185.dkr.ecr.ca-west-1.amazonaws.com
	–
Naher Osten (VAE)	759879836304.dkr.ecr.me-central-1.amazonaws.com
	601769779514.dkr.ecr.me-central-1.amazonaws.com
Europa (London)	602401143452.dkr.ecr.eu-west-2.amazonaws.com
	109118265657.dkr.ecr.eu-west-2.amazonaws.com
USA West (Nordkalifornien)	602401143452.dkr.ecr.us-west-1.amazonaws.com
	373421517865.dkr.ecr.us-west-1.amazonaws.com
USA Ost (Nord-Virginia)	602401143452.dkr.ecr.us-east-1.amazonaws.com
	031903291036.dkr.ecr.us-east-1.amazonaws.com
USA Ost (Ohio)	602401143452.dkr.ecr.us-east-2.amazonaws.com

AWS-Region	Amazon-ECR-Repository-URI
	591382732059.dkr.ecr.us-east-2.amazonaws.com
Europa (Irland)	602401143452.dkr.ecr.eu-west-1.amazonaws.com
	673884943994.dkr.ecr.eu-west-1.amazonaws.com
Südamerika (São Paulo)	602401143452.dkr.ecr.sa-east-1.amazonaws.com
	941219317354.dkr.ecr.sa-east-1.amazonaws.com
Europa (Stockholm)	602401143452.dkr.ecr.eu-north-1.amazonaws.com
	366771026645.dkr.ecr.eu-north-1.amazonaws.com
Europa (Frankfurt)	602401143452.dkr.ecr.eu-central-1.amazonaws.com
	409493279830.dkr.ecr.eu-central-1.amazonaws.com
Europa (Zürich)	900612956339.dkr.ecr.eu-central-2.amazonaws.com
	718440343717.dkr.ecr.eu-central-2.amazonaws.com
Asien-Pazifik (Singapur)	602401143452.dkr.ecr.ap-southeast-1.amazonaws.com
	584580519942.dkr.ecr.ap-southeast-1.amazonaws.com

AWS-Region	Amazon-ECR-Repository-URI
Asien-Pazifik (Sydney)	602401143452.dkr.ecr.ap-southeast-2.amazonaws.com
	011662287384.dkr.ecr.ap-southeast-2.amazonaws.com
Asien-Pazifik (Jakarta)	296578399912.dkr.ecr.ap-southeast-3.amazonaws.com
	617474730032.dkr.ecr.ap-southeast-3.amazonaws.com
Asien-Pazifik (Tokio)	602401143452.dkr.ecr.ap-northeast-1.amazonaws.com
	781592569369.dkr.ecr.ap-northeast-1.amazonaws.com
Asien-Pazifik (Seoul)	602401143452.dkr.ecr.ap-northeast-2.amazonaws.com
	732248494576.dkr.ecr.ap-northeast-2.amazonaws.com
Asien-Pazifik (Osaka)	602401143452.dkr.ecr.ap-northeast-3.amazonaws.com
	810724417379.dkr.ecr.ap-northeast-3.amazonaws.com
Asien-Pazifik (Hongkong)	800184023465.dkr.ecr.ap-east-1.amazonaws.com
	790429075973.dkr.ecr.ap-east-1.amazonaws.com
Middle East (Bahrain)	558608220178.dkr.ecr.me-south-1.amazonaws.com

AWS-Region	Amazon-ECR-Repository-URI
	541829937850.dkr.ecr.me-south-1.amazonaws.com
Europa (Milan)	590381155156.dkr.ecr.eu-south-1.amazonaws.com
	528450769569.dkr.ecr.eu-south-1.amazonaws.com
Europa (Spain)	455263428931.dkr.ecr.eu-south-2.amazonaws.com
	531047660167.dkr.ecr.eu-south-2.amazonaws.com
Afrika (Kapstadt)	877085696533.dkr.ecr.af-south-1.amazonaws.com
	379032919888.dkr.ecr.af-south-1.amazonaws.com
Asien-Pazifik (Melbourne)	491585149902.dkr.ecr.ap-southeast-4.amazonaws.com
	750462861327.dkr.ecr.ap-southeast-4.amazonaws.com
Israel (Tel Aviv)	066635153087.dkr.ecr.il-central-1.amazonaws.com
	292660727137.dkr.ecr.il-central-1.amazonaws.com
Asien-Pazifik (Malaysia)	151610086707.dkr.ecr.ap-southeast-5.amazonaws.com
Asien-Pazifik (Thailand)	121268973566.dkr.ecr.ap-southeast-7.amazonaws.com

AWS-Region	Amazon-ECR-Repository-URI
Mexiko (Zentral)	`730335286997.dkr.ecr.mx-central-1.amazonaws.com`
Asien-Pazifik (Taipeh)	`533267051163.dkr.ecr.ap-east-2.amazonaws.com`

ECR-Repository für EKS-Agenten Version 1.8.1 (eks.build.1)

Dieser Abschnitt enthält das Amazon ECR-Repository für die Amazon EKS-Agent-Version 1.8.1 (v1.8.1-eks-build.1). Wenn Sie v1.8.1-eks-build.1 verwenden, empfiehlt, zur Standard-Agentenversion zu wechseln, bei der es sich in der Regel um die neueste Agentenversion handelt. GuardDuty Identifizieren Sie dazu den neuesten Agenten von und führen Sie dann die Schritte unter ausVeröffentlichte Agentenversionen für Amazon EKS-Ressourcen. Manuelles Aktualisieren des Security Agents für Amazon EKS-Ressourcen

Die folgende Tabelle zeigt die Amazon ECR-Repository-URIs, auf denen die GuardDuty Security Agent-Version `1.8.1-eks-build.1` für Amazon EKS gehostet wird.

AWS-Region	Amazon-ECR-Repository-URI
USA West (Oregon)	`039403964562.dkr.ecr.us-west-2.amazonaws.com`
Europa (Paris)	`113643092156.dkr.ecr.eu-west-3.amazonaws.com`
Asien-Pazifik (Mumbai)	`610108029387.dkr.ecr.ap-south-1.amazonaws.com`
Asien-Pazifik (Hyderabad)	`618745550137.dkr.ecr.ap-south-2.amazonaws.com`
Kanada (Zentral)	`001188825231.dkr.ecr.ca-central-1.amazonaws.com`

AWS-Region	Amazon-ECR-Repository-URI
Naher Osten (VAE)	`601769779514.dkr.ecr.me-central-1.amazonaws.com`
Europa (London)	`109118265657.dkr.ecr.eu-west-2.amazonaws.com`
USA West (Nordkalifornien)	`373421517865.dkr.ecr.us-west-1.amazonaws.com`
USA Ost (Nord-Virginia)	`031903291036.dkr.ecr.us-east-1.amazonaws.com`
USA Ost (Ohio)	`591382732059.dkr.ecr.us-east-2.amazonaws.com`
Europa (Irland)	`673884943994.dkr.ecr.eu-west-1.amazonaws.com`
Südamerika (São Paulo)	`941219317354.dkr.ecr.sa-east-1.amazonaws.com`
Europa (Stockholm)	`366771026645.dkr.ecr.eu-north-1.amazonaws.com`
Europa (Frankfurt)	`409493279830.dkr.ecr.eu-central-1.amazonaws.com`
Europa (Zürich)	`718440343717.dkr.ecr.eu-central-2.amazonaws.com`
Asien-Pazifik (Singapur)	`584580519942.dkr.ecr.ap-southeast-1.amazonaws.com`
Asien-Pazifik (Sydney)	`011662287384.dkr.ecr.ap-southeast-2.amazonaws.com`
Asien-Pazifik (Jakarta)	`617474730032.dkr.ecr.ap-southeast-3.amazonaws.com`

AWS-Region	Amazon-ECR-Repository-URI
Asien-Pazifik (Tokio)	`781592569369.dkr.ecr.ap-northeast-1.amazonaws.com`
Asien-Pazifik (Seoul)	`732248494576.dkr.ecr.ap-northeast-2.amazonaws.com`
Asien-Pazifik (Osaka)	`810724417379.dkr.ecr.ap-northeast-3.amazonaws.com`
Asien-Pazifik (Hongkong)	`790429075973.dkr.ecr.ap-east-1.amazonaws.com`
Middle East (Bahrain)	`541829937850.dkr.ecr.me-south-1.amazonaws.com`
Europa (Milan)	`528450769569.dkr.ecr.eu-south-1.amazonaws.com`
Europa (Spain)	`531047660167.dkr.ecr.eu-south-2.amazonaws.com`
Afrika (Kapstadt)	`379032919888.dkr.ecr.af-south-1.amazonaws.com`
Asien-Pazifik (Melbourne)	`750462861327.dkr.ecr.ap-southeast-4.amazonaws.com`
Israel (Tel Aviv)	`292660727137.dkr.ecr.il-central-1.amazonaws.com`

ECR-Repository für Agenten an GuardDuty AWS Fargate (Nur Amazon ECS)

Als Voraussetzung für die Nutzung von Runtime Monitoring for Amazon ECS-Fargate müssen Sie: Voraussetzungen für den Zugriff auf Container-Images Das GuardDuty Agenten-Sidecar-Container-Image wird in Amazon ECR gespeichert, und die Bildebenen werden in Amazon S3 gespeichert.

Weitere Informationen finden Sie unter So funktioniert Runtime Monitoring mit Fargate (nur Amazon ECS).

Die folgende Tabelle zeigt die Amazon ECR-Repositorys, für die jeweils der GuardDuty Agent gehostet wird AWS Fargate (nur Amazon ECS). AWS-Region

AWS-Region	Amazon-ECR-Repository-URI
USA West (Oregon)	`733349766148.dkr.ecr.us-west-2.amazonaws.com/aws-guardduty-agent-fargate`
Europa (Paris)	`665651866788.dkr.ecr.eu-west-3.amazonaws.com/aws-guardduty-agent-fargate`
Asien-Pazifik (Mumbai)	`251508486986.dkr.ecr.ap-south-1.amazonaws.com/aws-guardduty-agent-fargate`
Asien-Pazifik (Hyderabad)	`950823858135.dkr.ecr.ap-south-2.amazonaws.com/aws-guardduty-agent-fargate`
Kanada (Zentral)	`354763396469.dkr.ecr.ca-central-1.amazonaws.com/aws-guardduty-agent-fargate`
Naher Osten (VAE)	`000014521398.dkr.ecr.me-central-1.amazonaws.com/aws-guardduty-agent-fargate`
Europa (London)	`892757235363.dkr.ecr.eu-west-2.amazonaws.com/aws-guardduty-agent-fargate`
USA West (Nordkalifornien)	`684579721401.dkr.ecr.us-west-1.amazonaws.com/aws-guardduty-agent-fargate`

AWS-Region	Amazon-ECR-Repository-URI
USA Ost (Nord-Virginia)	`593207742271.dkr.ecr.us-east-1.amazonaws.com/aws-guardduty-agent-fargate`
USA Ost (Ohio)	`307168627858.dkr.ecr.us-east-2.amazonaws.com/aws-guardduty-agent-fargate`
Europa (Irland)	`694911143906.dkr.ecr.eu-west-1.amazonaws.com/aws-guardduty-agent-fargate`
Südamerika (São Paulo)	`758426053663.dkr.ecr.sa-east-1.amazonaws.com/aws-guardduty-agent-fargate`
Europa (Stockholm)	`591436053604.dkr.ecr.eu-north-1.amazonaws.com/aws-guardduty-agent-fargate`
Europa (Frankfurt)	`323658145986.dkr.ecr.eu-central-1.amazonaws.com/aws-guardduty-agent-fargate`
Europa (Zürich)	`529164026651.dkr.ecr.eu-central-2.amazonaws.com/aws-guardduty-agent-fargate`
Asien-Pazifik (Singapur)	`174946120834.dkr.ecr.ap-southeast-1.amazonaws.com/aws-guardduty-agent-fargate`
Asien-Pazifik (Sydney)	`005257825471.dkr.ecr.ap-southeast-2.amazonaws.com/aws-guardduty-agent-fargate`

AWS-Region	Amazon-ECR-Repository-URI
Asien-Pazifik (Jakarta)	510637619217.dkr.ecr.ap-southeast-3.amazonaws.com/aws-guardduty-agent-fargate
Asien-Pazifik (Tokio)	533107202818.dkr.ecr.ap-northeast-1.amazonaws.com/aws-guardduty-agent-fargate
Asien-Pazifik (Seoul)	914738172881.dkr.ecr.ap-northeast-2.amazonaws.com/aws-guardduty-agent-fargate
Asien-Pazifik (Osaka)	273192626886.dkr.ecr.ap-northeast-3.amazonaws.com/aws-guardduty-agent-fargate
Asien-Pazifik (Hongkong)	258348409381.dkr.ecr.ap-east-1.amazonaws.com/aws-guardduty-agent-fargate
Middle East (Bahrain)	536382113932.dkr.ecr.me-south-1.amazonaws.com/aws-guardduty-agent-fargate
Europa (Milan)	266869475730.dkr.ecr.eu-south-1.amazonaws.com/aws-guardduty-agent-fargate
Europa (Spain)	919611009337.dkr.ecr.eu-south-2.amazonaws.com/aws-guardduty-agent-fargate
Afrika (Kapstadt)	197869348890.dkr.ecr.af-south-1.amazonaws.com/aws-guardduty-agent-fargate

AWS-Region	Amazon-ECR-Repository-URI
Asien-Pazifik (Melbourne)	`251357961535.dkr.ecr.ap-southeast-4.amazonaws.com/aws-guardduty-agent-fargate`
Israel (Tel Aviv)	`870907303882.dkr.ecr.il-central-1.amazonaws.com/aws-guardduty-agent-fargate`
Asien-Pazifik (Malaysia)	`156041399949.dkr.ecr.ap-southeast-5.amazonaws.com/aws-guardduty-agent-fargate`
Asien-Pazifik (Thailand)	`054037130133.dkr.ecr.ap-southeast-7.amazonaws.com/aws-guardduty-agent-fargate`
Kanada West (Calgary)	`339712888787.dkr.ecr.ca-west-1.amazonaws.com/aws-guardduty-agent-fargate`
Mexiko (Zentral)	`311141559934.dkr.ecr.mx-central-1.amazonaws.com/aws-guardduty-agent-fargate`
Asien-Pazifik (Taipeh)	`259886477082.dkr.ecr.ap-east-2.amazonaws.com/aws-guardduty-agent-fargate`

ECR-Repository für GuardDuty Agenten auf Bottlerocket ECS-EC2

Auf Bottlerocket Amazon ECS-Amazon EC2-Instances wird der Security Agent als Host-Container ausgeführt. GuardDuty Das Agent-Container-Image wird in Amazon ECR gehostet. Informationen zu den Voraussetzungen, einschließlich Netzwerkkonnektivität und erforderlichen IAM-Berechtigungen, finden Sie unter. Voraussetzungen für die ECS-EC2 Bottlerocket-Unterstützung Das Instanzprofil muss die `AmazonSSMManagedInstanceCore` und `AmazonEC2ContainerRegistryReadOnly` verwalteten Richtlinien enthalten.

Die folgende Tabelle zeigt die Amazon ECR-Repositorys, die jeweils den GuardDuty Agenten für Amazon ECS-Amazon EC2 Bottlerocket-Instances hosten. AWS-Region

AWS-Region	Amazon-ECR-Repository-URI
USA Ost (Nord-Virginia)	`593207742271.dkr.ecr.us-east-1.amazonaws.com/aws-guardduty-agent-ecs-ec2`
USA Ost (Ohio)	`307168627858.dkr.ecr.us-east-2.amazonaws.com/aws-guardduty-agent-ecs-ec2`
USA West (Nordkalifornien)	`684579721401.dkr.ecr.us-west-1.amazonaws.com/aws-guardduty-agent-ecs-ec2`
US West (Oregon)	`733349766148.dkr.ecr.us-west-2.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Europa (Irland)	`694911143906.dkr.ecr.eu-west-1.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Europa (London)	`892757235363.dkr.ecr.eu-west-2.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Europa (Paris)	`665651866788.dkr.ecr.eu-west-3.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Europa (Frankfurt)	`323658145986.dkr.ecr.eu-central-1.amazonaws.com/aws-guardduty-agent-ecs-ec2`

AWS-Region	Amazon-ECR-Repository-URI
Europa (Zürich)	`529164026651.dkr.ecr.eu-central-2.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Europa (Stockholm)	`591436053604.dkr.ecr.eu-north-1.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Europa (Milan)	`266869475730.dkr.ecr.eu-south-1.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Europa (Spain)	`919611009337.dkr.ecr.eu-south-2.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Asien-Pazifik (Tokio)	`533107202818.dkr.ecr.ap-northeast-1.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Asien-Pazifik (Seoul)	`914738172881.dkr.ecr.ap-northeast-2.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Asien-Pazifik (Osaka)	`273192626886.dkr.ecr.ap-northeast-3.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Asien-Pazifik (Singapur)	`174946120834.dkr.ecr.ap-southeast-1.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Asien-Pazifik (Sydney)	`005257825471.dkr.ecr.ap-southeast-2.amazonaws.com/aws-guardduty-agent-ecs-ec2`

AWS-Region	Amazon-ECR-Repository-URI
Asien-Pazifik (Jakarta)	510637619217.dkr.ecr.ap-southeast-3.amazonaws.com/aws-guardduty-agent-ecs-ec2
Asien-Pazifik (Melbourne)	251357961535.dkr.ecr.ap-southeast-4.amazonaws.com/aws-guardduty-agent-ecs-ec2
Asien-Pazifik (Mumbai)	251508486986.dkr.ecr.ap-south-1.amazonaws.com/aws-guarduty-agent-ecs-ec2
Asien-Pazifik (Hyderabad)	950823858135.dkr.ecr.ap-south-2.amazonaws.com/aws-guarduty-agent-ecs-ec2
Asien-Pazifik (Hongkong)	258348409381.dkr.ecr.ap-east-1.amazonaws.com/aws-guardduty-agent-ecs-ec2
Kanada (Zentral)	354763396469.dkr.ecr.ca-central-1.amazonaws.com/aws-guardduty-agent-ecs-ec2
Kanada West (Calgary)	339712888787.dkr.ecr.ca-west-1.amazonaws.com/aws-guardduty-agent-ecs-ec2
Südamerika (São Paulo)	758426053663.dkr.ecr.sa-east-1.amazonaws.com/aws-guardduty-agent-ecs-ec2
Middle East (Bahrain)	536382113932.dkr.ecr.me-south-1.amazonaws.com/aws-guarduty-agent-ecs-ec2

AWS-Region	Amazon-ECR-Repository-URI
Naher Osten (VAE)	`000014521398.dkr.ecr.me-central-1.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Afrika (Kapstadt)	`197869348890.dkr.ecr.af-south-1.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Israel (Tel Aviv)	`870907303882.dkr.ecr.il-central-1.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Asien-Pazifik (Malaysia)	`156041399949.dkr.ecr.ap-southeast-5.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Asien-Pazifik (Thailand)	`054037130133.dkr.ecr.ap-southeast-7.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Mexiko (Zentral)	`311141559934.dkr.ecr.mx-central-1.amazonaws.com/aws-guardduty-agent-ecs-ec2`
Asien-Pazifik (Taipeh)	`259886477082.dkr.ecr.ap-east-2.amazonaws.com/aws-guardduty-agent-ecs-ec2`

Zwei Security Agents auf demselben zugrunde liegenden Host

Amazon EC2-Instances können mehrere Arten von Workloads unterstützen. Wenn Sie einen automatisierten Sicherheitsagenten auf einer Amazon EC2-Instance konfigurieren, verfügt dieselbe EC2-Instance möglicherweise über EKS über einen anderen Sicherheitsagenten.

-Übersicht

Stellen Sie sich ein Szenario vor, in dem Sie Runtime Monitoring aktiviert haben. Jetzt aktivieren Sie den automatisierten Agenten für Amazon EKS über GuardDuty. Sie haben auch den automatisierten Agenten für Amazon EC2 aktiviert. Es kann vorkommen, dass derselbe zugrundeliegende Host mit zwei Sicherheitsagenten installiert wird — einer für Amazon EKS und der andere für Amazon EC2. Dies könnte dazu führen, dass zwei Security Agents auf demselben Host laufen, Laufzeitereignisse sammeln und an GuardDuty sie senden und möglicherweise doppelte Ergebnisse generieren.

Auswirkung

- Wenn mehr als ein Security Agent auf demselben Host läuft, kann es sein, dass Ihr Konto doppelt so viel CPU- und Speicherverarbeitungsbedarf hat. Informationen zu den CPU- und Speicherlimits für jeden Ressourcentyp finden Sie Voraussetzungen für die jeweilige Ressource.
- GuardDuty hat die Funktion zur Laufzeitüberwachung so konzipiert, dass Ihr Konto nur für einen Stream von Laufzeitereignissen belastet wird, selbst wenn sich zwei Security Agents, die Laufzeitereignisse von demselben zugrundeliegenden Host sammeln, überschneiden.

Wie GuardDuty geht man mit mehreren Agenten um

GuardDuty erkennt, wenn zwei Security Agents auf demselben Host laufen, und bestimmt nur einen von ihnen als Security Agent, der aktiv Laufzeitereignisse sammelt. Der zweite Agent verbraucht nur minimale Systemressourcen, um jegliche Beeinträchtigung der Leistung Ihrer Anwendungen zu verhindern.

GuardDuty berücksichtigt die folgenden Szenarien:

- Wenn eine EC2-Instance sowohl in den Zuständigkeitsbereich von Amazon EKS- als auch von Amazon EC2-Sicherheitsagenten fällt, hat der EKS-Sicherheitsagent Vorrang. Dies gilt nur, wenn Sie den Security Agent v1.1.0 oder höher für Amazon EC2 verwenden. Ältere Agentenversionen werden weiterhin ausgeführt und erfassen Laufzeitereignisse, da ältere Agentenversionen von der Priorisierung nicht betroffen sind.
- Wenn sowohl Amazon EKS als auch Amazon EC2 über GuardDuty verwaltete Sicherheitsagenten verfügen und Ihre Amazon EC2-Instance ebenfalls SSM-verwaltet wird, werden beide Sicherheitsagenten auf Host-Ebene installiert. Sobald die Agents installiert sind, wird GuardDuty entschieden, welcher Security Agent weiter ausgeführt wird. Wenn beide Security Agents laufen, erfasst irgendwann nur einer von ihnen Laufzeitereignisse.

- Wenn die Security Agents, die sowohl mit EC2 als auch mit EKS verknüpft sind, gleichzeitig ausgeführt werden, werden GuardDuty möglicherweise nur während des Überschneidungszeitraums doppelte Ergebnisse generiert.

  Dies kann passieren, wenn:

  - Die Sicherheitsagenten sowohl für EC2 als auch für EKS werden über GuardDuty (automatisch) konfiguriert, oder
  - Ihre Amazon EKS-Ressource verfügt über einen automatisierten Sicherheitsagenten.
- Wenn der EKS Security Agent bereits läuft und Sie den EC2 Security Agent manuell auf demselben zugrunde liegenden Host bereitstellen und alle Voraussetzungen erfüllen, wird GuardDuty möglicherweise kein zweiter Security Agent installiert.

EKS-Laufzeitüberwachung in GuardDuty

EKS Runtime Monitoring deckt während der Laufzeit die Erkennung von Bedrohungen für Amazon Elastic Kubernetes Service (Amazon EKS) -Knoten und Container in Ihrer AWS Umgebung ab. EKS Runtime Monitoring verwendet einen GuardDuty Sicherheitsagenten, der einzelne EKS-Workloads wie Dateizugriff, Prozessausführung und Netzwerkverbindungen zur Laufzeit transparenter macht. Der GuardDuty Security Agent hilft dabei, bestimmte Container in Ihren EKS-Clustern zu GuardDuty identifizieren, die potenziell gefährdet sind. Er kann auch Versuche erkennen, Rechte von einem einzelnen Container auf den zugrunde liegenden EC2-Host und die gesamte Umgebung auszudehnen. AWS

Mit der Verfügbarkeit von Runtime Monitoring GuardDuty hat das Konsolenerlebnis für EKS Runtime Monitoring in Runtime Monitoring konsolidiert. GuardDuty migriert Ihre EKS Runtime Monitoring-Einstellungen nicht automatisch in Ihrem Namen. Dies erfordert eine Aktion auf Ihrer Seite. Wenn Sie weiterhin nur EKS Runtime Monitoring verwenden möchten, können Sie die APIs verwenden oder AWS CLI den vorhandenen Konfigurationsstatus für EKS Runtime Monitoring überprüfen und aktualisieren. GuardDuty empfiehlt Migrieren von EKS Runtime Monitoring zu Runtime Monitoring jedoch, Runtime Monitoring zur Überwachung Ihrer Amazon EKS-Cluster zu verwenden.

Themen

- Konfiguration von EKS Runtime Monitoring für Umgebungen mit mehreren Konten (API)
- Konfiguration von EKS Runtime Monitoring für ein eigenständiges Konto (API)
- Migrieren von EKS Runtime Monitoring zu Runtime Monitoring

Konfiguration von EKS Runtime Monitoring für Umgebungen mit mehreren Konten (API)

In Umgebungen mit mehreren Konten kann nur das delegierte GuardDuty Administratorkonto EKS Runtime Monitoring für die Mitgliedskonten aktivieren oder deaktivieren und die GuardDuty Agentenverwaltung für die EKS-Cluster verwalten, die zu den Mitgliedskonten in ihrer Organisation gehören. Die GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Das Konto des delegierten GuardDuty Administratorkontos verwaltet ihre Mitgliedskonten mithilfe von AWS Organizations. Weitere Informationen zu Umgebungen mit mehreren Konten finden Sie unter Verwaltung mehrerer Konten.

Konfiguration von EKS Runtime Monitoring für ein delegiertes Administratorkonto GuardDuty

Dieser Abschnitt enthält Schritte zur Konfiguration von EKS Runtime Monitoring und zur Verwaltung des GuardDuty Security Agents für die EKS-Cluster, die zum delegierten GuardDuty Administratorkonto gehören.

Auf der Grundlage von Ansätze zur Verwaltung von GuardDuty Sicherheitsagenten in Amazon EKS-Clustern können Sie einen bevorzugten Ansatz wählen und die in der folgenden Tabelle aufgeführten Schritte ausführen.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Verwalten Sie den Security Agent über GuardDuty (Überwachen Sie alle EKS-Cluster)	Führen Sie die updateDetector-API aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den `features`-Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als `ENABLED` übergeben. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster in Ihrem Konto. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Detektor-ID verwenden. Um die `detectorId` für Ihr Konto und Ihre aktuelle Region zu

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	finden, besuchen Sie die Einstellungsseite in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. Das folgende Beispiel aktiviert sowohl EKS_RUNTIME_MONITORING als auch EKS_ADDON_MANAGEMENT : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] }]'`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Alle EKS-Cluster überwachen, jedoch einige davon ausschließen (mithilfe des Ausschluss-Tags)	1. Fügen Sie dem EKS-Cluster, den Sie von der Überwachung ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar ist `GuardDuty Managed -false`. Weitere Informationen zum Hinzufügen eines Tags finden Sie unter Arbeiten mit Tags mithilfe der CLI, API oder eksctl im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2:CreateTags* durch `eks:TagResource`. • Ersetzen Sie *ec2:DeleteTags* durch `eks:UntagResource`. • Ersetzen Sie *access-project* durch `GuardDuty Managed` • *123456789012* Ersetzen Sie durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	3.

> **Note**
>
> Fügen Sie Ihrem EKS-Cluster immer das Ausschluss-Tag hinzu, bevor Sie den Wert `STATUS` von `EKS_RUNTIME_MONITORING` auf setzen. `ENABLED` Andernfalls wird der GuardDuty Security Agent auf allen EKS-Clusts in Ihrem Konto bereitgestellt.

Führen Sie die updateDetector-API aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den `features`-Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als `ENABLED` übergeben.

Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein.

GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster, die nicht von der Überwachung ausgeschlossen wurden.

Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Detektor-ID verwenden. Um die `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, besuchen Sie die Einstellungsseite in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus.

Das folgende Beispiel aktiviert sowohl `EKS_RUNTIME_MONITORING` als auch `EKS_ADDON_MANAGEMENT` :

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	`aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] }]'`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Ausgewählte EKS-Cluster überwachen (mithilfe des Einschließen-Tags)	1. Fügen Sie dem EKS-Cluster ein Tag hinzu, das Sie in die Überwachung einbeziehen möchten. Das Schlüssel-Wert-Paar ist `GuardDutyManaged -true`. Weitere Informationen zum Hinzufügen eines Tags finden Sie unter Arbeiten mit Tags mithilfe der CLI, API oder eksctl im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2:CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2:DeleteTags* durch `eks:UntagResource` . • Ersetzen *access-project* durch `GuardDutyManaged` • *123456789012* Ersetzen Sie durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Führen Sie die updateDetector-API aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	`features`-Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als `ENABLED` übergeben. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster, die mit dem `true` Paar `GuardDutyManaged` — markiert wurden. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Detektor-ID verwenden. Um die `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, besuchen Sie die Einstellungsseite in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITORING` und deaktiviert `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] }]'`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Den Sicherheitsagent manuell verwalten	1. Führen Sie die updateDetector-API aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den `features`-Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als `ENABLED` übergeben. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Detektor-ID verwenden. Um die `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, besuchen Sie die Einstellungsseite in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITORING` und deaktiviert `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] }]'` 2. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Sicherheitsagenten für den Amazon EKS-Cluster.

Auto-enable EKS-Laufzeitüberwachung für alle Mitgliedskonten

Dieser Abschnitt enthält Schritte zur Aktivierung von EKS Runtime Monitoring und zur Verwaltung des Security Agents für alle Mitgliedskonten. Dazu gehören das delegierte GuardDuty Administratorkonto, bestehende Mitgliedskonten und die neuen Konten, die der Organisation beitreten.

Auf der Grundlage von Ansätze zur Verwaltung von GuardDuty Sicherheitsagenten in Amazon EKS-Clustern können Sie einen bevorzugten Ansatz wählen und die in der folgenden Tabelle aufgeführten Schritte ausführen.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Verwalten Sie den Security Agent über GuardDuty (Überwachen Sie alle EKS-Cluster)	Um EKS Runtime Monitoring selektiv für Ihre Mitgliedskonten zu aktivieren, führen Sie den updateMemberDetectors API-Vorgang mit Ihrem eigenen *detector ID* aus. Stellen Sie den Status für EKS_ADDON_MANAGEMENT als ENABLED ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster in Ihrem Konto. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Detektor-ID verwenden. Um die detectorId für Ihr Konto und Ihre aktuelle Region zu finden, besuchen Sie die Einstellungsseite in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. Das folgende Beispiel aktiviert sowohl EKS_RUNTIME_MONITORING als auch EKS_ADDON_MANAGEMENT : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] }]'`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	> **Note** > Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind. Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Alle EKS-Cluster überwachen, jedoch einige davon ausschließen (mithilfe des Ausschluss-Tags)	1. Fügen Sie dem EKS-Cluster, den Sie von der Überwachung ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar ist `GuardDutyManaged -false`. Weitere Informationen zum Hinzufügen eines Tags finden Sie unter Arbeiten mit Tags mithilfe der CLI, API oder eksctl im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *`ec2:CreateTags`* durch `eks:TagResource` . • Ersetzen Sie *`ec2:DeleteTags`* durch `eks:UntagResource` . • Ersetzen Sie *`access-project`* durch `GuardDutyManaged` • *`123456789012`* Ersetzen Sie durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	3.

> **Note**
>
> Fügen Sie Ihrem EKS-Cluster immer das Ausschluss-Tag hinzu, bevor Sie den Wert `STATUS` von `EKS_RUNTIME_MONITORING` auf setzen. `ENABLED` Andernfalls wird der GuardDuty Security Agent auf allen EKS-Clustern in Ihrem Konto bereitgestellt.

Führen Sie die updateDetector-API aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den `features`-Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als `ENABLED` übergeben.

Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein.

GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster, die nicht von der Überwachung ausgeschlossen wurden.

Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Detektor-ID verwenden. Um die `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, besuchen Sie die Einstellungsseite in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus.

Das folgende Beispiel aktiviert sowohl `EKS_RUNTIME_MONITORING` als auch `EKS_ADDON_MANAGEMENT` :

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0    --account-
```

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte

```
ids 111122223333  --features '[{"Name" : "EKS_RUNT
IME_MONITORING", "Status" : "  ENABLED", "Addition
alConfiguration" : [{"Name" : "EKS_ADDON_MANAGEM
ENT", "Status" : " ENABLED"}] }]'
```

> **Note**
>
> Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Ausgewählte EKS-Cluster überwachen (mithilfe des Einschließen-Tags)	1. Fügen Sie dem EKS-Cluster ein Tag hinzu, das Sie in die Überwachung einbeziehen möchten. Das Schlüssel-Wert-Paar ist `GuardDutyManaged -true`. Weitere Informationen zum Hinzufügen eines Tags finden Sie unter Arbeiten mit Tags mithilfe der CLI, API oder eksctl im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2:CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2:DeleteTags* durch `eks:UntagResource` . • Ersetzen *access-project* durch `GuardDutyManaged` • *123456789012* Ersetzen Sie durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Führen Sie die updateDetector-API aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den `features`-Objektna

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	men als `EKS_RUNTIME_MONITORING` und den Status als `ENABLED` übergeben. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster, die mit dem `true` Paar `GuardDutyManaged` — markiert wurden. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Detektor-ID verwenden. Um die `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, besuchen Sie die Einstellungsseite in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITORING` und deaktiviert `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] }]'` **Note** Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Den Sicherheitsagent manuell verwalten	1. Führen Sie die updateDetector-API aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den `features`-Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als `ENABLED` übergeben. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Detektor-ID verwenden. Um die `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, besuchen Sie die Einstellungsseite in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITORING` und deaktiviert `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] } ]'` 2. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Sicherheitsagenten für den Amazon EKS-Cluster.

Konfiguration der EKS-Laufzeit-Überwachung für alle vorhandenen aktiven Mitgliedskonten

Dieser Abschnitt enthält die Schritte zur Aktivierung von EKS Runtime Monitoring und zur Verwaltung des GuardDuty Security Agents für bestehende aktive Mitgliedskonten in Ihrer Organisation.

Auf der Grundlage von Ansätze zur Verwaltung von GuardDuty Sicherheitsagenten in Amazon EKS-Clustern können Sie einen bevorzugten Ansatz wählen und die in der folgenden Tabelle aufgeführten Schritte ausführen.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Verwalten Sie den Security Agent über GuardDuty (Überwachen Sie alle EKS-Cluster)	Um EKS Runtime Monitoring selektiv für Ihre Mitgliedskonten zu aktivieren, führen Sie den updateMemberDetectors API-Vorgang mit Ihrem eigenen *detector ID* aus. Stellen Sie den Status für EKS_ADDON_MANAGEMENT als ENABLED ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster in Ihrem Konto. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Detektor-ID verwenden. Um die detectorId für Ihr Konto und Ihre aktuelle Region zu finden, besuchen Sie die Einstellungsseite in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. Das folgende Beispiel aktiviert sowohl EKS_RUNTIME_MONITORING als auch EKS_ADDON_MANAGEMENT : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] }]'`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	> **Note** > Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind. Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Alle EKS-Cluster überwachen, jedoch einige davon ausschließen (mithilfe des Ausschluss-Tags)	1. Fügen Sie dem EKS-Cluster, den Sie von der Überwachung ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar ist `GuardDutyManaged -false`. Weitere Informationen zum Hinzufügen eines Tags finden Sie unter Arbeiten mit Tags mithilfe der CLI, API oder eksctl im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2:CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2:DeleteTags* durch `eks:UntagResource` . • Ersetzen Sie *access-project* durch `GuardDutyManaged` • *123456789012* Ersetzen Sie durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	3.

> **Note**
>
> Fügen Sie Ihrem EKS-Cluster immer das Ausschluss-Tag hinzu, bevor Sie den Wert `STATUS` von `EKS_RUNTIME_MONITORING` auf setzen. `ENABLED` Andernfalls wird der GuardDuty Security Agent auf allen EKS-Clustern in Ihrem Konto bereitgestellt.

Um EKS Runtime Monitoring selektiv für Ihre Mitgliedskonten zu aktivieren, führen Sie den updateMemberDetectors API-Vorgang mit Ihrem eigenen *`detector ID`* aus.

Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein.

GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster, die nicht von der Überwachung ausgeschlossen wurden.

Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Detektor-ID verwenden. Um die `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, besuchen Sie die Einstellungsseite in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus.

Das folgende Beispiel aktiviert sowohl `EKS_RUNTIME_MONITORING` als auch `EKS_ADDON_MANAGEMENT` :

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0    --account-
ids 111122223333  --features '[{"Name" : "EKS_RUNT
IME_MONITORING", "Status" : "  ENABLED", "Addition
```

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte

```
alConfiguration" : [{"Name" : "EKS_ADDON_MANAGEM
ENT", "Status" : " ENABLED"}] }]'
```

> **Note**
>
> Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Ausgewählte EKS-Cluster überwachen (mithilfe des Einschließen-Tags)	1. Fügen Sie dem EKS-Cluster ein Tag hinzu, das Sie in die Überwachung einbeziehen möchten. Das Schlüssel-Wert-Paar ist `GuardDutyManaged -true`. Weitere Informationen zum Hinzufügen eines Tags finden Sie unter Arbeiten mit Tags mithilfe der CLI, API oder eksctl im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2:CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2:DeleteTags* durch `eks:UntagResource` . • Ersetzen *access-project* durch `GuardDutyManaged` • *123456789012* Ersetzen Sie durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte

3. Um EKS Runtime Monitoring selektiv für Ihre Mitgliedskonten zu aktivieren, führen Sie den updateMemberDetectors API-Vorgang mit Ihrem eigenen *`detector ID`* aus.

   Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein.

   GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster, die mit dem `true` Paar `GuardDutyManaged` — markiert wurden.

   Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Detektor-ID verwenden. Um die `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, besuchen Sie die Einstellungsseite in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus.

   Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITORING` und deaktiviert `EKS_ADDON_MANAGEMENT` :

   ```
   aws guardduty update-member-detectors --detector-
   id 12abc34d567e8fa901bc2d34e56789f0    --account-
   ids 111122223333  --features '[{"Name" : "EKS_RUNT
   IME_MONITORING", "Status" : "  ENABLED", "Addition
   alConfiguration" : [{"Name" : "EKS_ADDON_MANAGEM
   ENT", "Status" : " DISABLED"}] }]'
   ```

   > **Note**
   >
   > Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.
Den Sicherheitsagent manuell verwalten	1. Um EKS Runtime Monitoring für Ihre Mitgliedskonten selektiv zu aktivieren, führen Sie den updateMemberDetectors API-Vorgang mit Ihrem eigenen *`detector ID`* aus. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Detektor-ID verwenden. Um die `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, besuchen Sie die Einstellungsseite in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITORING` und deaktiviert `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] } ]'` 2. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Sicherheitsagenten für den Amazon EKS-Cluster.

Auto-enable EKS Runtime Monitoring für neue Mitglieder

Das delegierte GuardDuty Administratorkonto kann EKS Runtime Monitoring automatisch aktivieren und einen Ansatz für die Verwaltung des GuardDuty Security Agents für neue Konten auswählen, die Ihrer Organisation beitreten.

Auf der Grundlage von Ansätze zur Verwaltung von GuardDuty Sicherheitsagenten in Amazon EKS-Clustern können Sie einen bevorzugten Ansatz wählen und die in der folgenden Tabelle aufgeführten Schritte ausführen.

Bevorzugter Ansatz zur Verwaltung des Security Agents GuardDuty	Schritte
Verwalten Sie den Security Agent über GuardDuty (Überwachen Sie alle EKS-Cluster)	Um EKS Runtime Monitoring selektiv für Ihre neuen Konten zu aktivieren, rufen Sie den UpdateOrganizationConfiguration API-Vorgang mit Ihrem eigenen auf. *detector ID* Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster in Ihrem Konto. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Detektor-ID verwenden. Um die `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, besuchen Sie die Einstellungsseite in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. Im folgenden Beispiel werden beide Optionen `EKS_RUNTIME_MONITORING` und `EKS_ADDON_MANAGEMENT` für ein einzelnes Konto aktiviert. Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind. Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://c

Bevorzugter Ansatz zur Verwaltung des Security Agents GuardDuty	Schritte
	onsole.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId` `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] }]'` Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des Security Agents GuardDuty	Schritte
Alle EKS-Cluster überwachen, jedoch einige davon ausschließen (mithilfe des Ausschluss-Tags)	1. Fügen Sie dem EKS-Cluster, den Sie von der Überwachung ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar ist `GuardDuty Managed -false`. Weitere Informationen zum Hinzufügen eines Tags finden Sie unter Arbeiten mit Tags mithilfe der CLI, API oder eksctl im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2:CreateTags* durch `eks:TagResource`. • Ersetzen Sie *ec2:DeleteTags* durch `eks:UntagResource`. • Ersetzen Sie *access-project* durch `GuardDuty Managed` • *123456789012* Ersetzen Sie durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Bevorzugter Ansatz zur Verwaltung des Security Agents GuardDuty	Schritte
	3.

> **Note**
>
> Fügen Sie Ihrem EKS-Cluster immer das Ausschluss-Tag hinzu, bevor Sie den Wert `STATUS` von `EKS_RUNTIME_MONITORING` auf setzen. `ENABLED` Andernfalls wird der GuardDuty Security Agent auf allen EKS-Clust ern in Ihrem Konto bereitgestellt.

Um EKS Runtime Monitoring selektiv für Ihre neuen Konten zu aktivieren, rufen Sie den UpdateOrganization Configuration API-Vorgang mit Ihrem eigenen auf. *`detector ID`*

Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein.

GuardDuty verwaltet die Bereitstellung und Aktualisi erung des Security Agents für alle Amazon EKS-Clust er, die nicht von der Überwachung ausgeschlossen wurden.

Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Detektor-ID verwenden . Um die `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, besuchen Sie die Einstellungsseite in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus.

Im folgenden Beispiel werden beide Optionen `EKS_RUNTIME_MONITORING` und `EKS_ADDON _MANAGEMENT` für ein einzelnes Konto aktiviert. Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

Bevorzugter Ansatz zur Verwaltung des Security Agents GuardDuty	Schritte
	Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId` `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] }]'` Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des Security Agents GuardDuty	Schritte
Ausgewählte EKS-Cluster überwachen (mithilfe des Einschließen-Tags)	1. Fügen Sie dem EKS-Cluster ein Tag hinzu, das Sie in die Überwachung einbeziehen möchten. Das Schlüssel-Wert-Paar ist `GuardDutyManaged -true`. Weitere Informationen zum Hinzufügen eines Tags finden Sie unter Arbeiten mit Tags mithilfe der CLI, API oder eksctl im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2:CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2:DeleteTags* durch `eks:UntagResource` . • Ersetzen *access-project* durch `GuardDutyManaged` • *123456789012* Ersetzen Sie durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Um EKS Runtime Monitoring selektiv für Ihre neuen Konten zu aktivieren, rufen Sie den UpdateOrganization

Bevorzugter Ansatz zur Verwaltung des Security Agents GuardDuty	Schritte
	Configuration API-Vorgang mit Ihrem eigenen auf. *detector ID* Stellen Sie den Status für EKS_ADDON_MANAGEMENT als DISABLED ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster, die mit dem GuardDutyManaged - true Paar markiert wurden. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Detektor-ID verwenden. Um die detectorId für Ihr Konto und Ihre aktuelle Region zu finden, besuchen Sie die Einstellungsseite in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. Das folgende Beispiel aktiviert EKS_RUNTIME_MONITORING und deaktiviert EKS_ADDON_MANAGEMENT für ein einzelnes Konto. Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind. Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. detectorId `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfigu`

Bevorzugter Ansatz zur Verwaltung des Security Agents GuardDuty	Schritte
	ration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] }]' Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des Security Agents GuardDuty	Schritte
Den Sicherheitsagent manuell verwalten	1. Um EKS Runtime Monitoring für Ihre neuen Konten selektiv zu aktivieren, rufen Sie den UpdateOrganizationConfiguration API-Vorgang mit Ihrem eigenen auf. *detector ID* Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Detektor-ID verwenden. Um die `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, besuchen Sie die Einstellungsseite in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITORING` und deaktiviert `EKS_ADDON_MANAGEMENT` für ein einzelnes Konto. Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind. Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId` `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] }]'`

Bevorzugter Ansatz zur Verwaltung des Security Agents GuardDuty	Schritte
	Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt. 2. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Sicherheitsagenten für den Amazon EKS-Cluster.

EKS-Laufzeit-Überwachung für einzelne aktive Mitgliedskonten aktivieren

Dieser Abschnitt enthält die Schritte zur Konfiguration von EKS Runtime Monitoring und zur Verwaltung des Security Agents für einzelne aktive Mitgliedskonten.

Auf der Grundlage von Ansätze zur Verwaltung von GuardDuty Sicherheitsagenten in Amazon EKS-Clustern können Sie einen bevorzugten Ansatz wählen und die in der folgenden Tabelle aufgeführten Schritte ausführen.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Verwalten Sie den Security Agent über GuardDuty (Überwachen Sie alle EKS-Cluster)	Um EKS Runtime Monitoring selektiv für Ihre Mitgliedskonten zu aktivieren, führen Sie den updateMemberDetectors API-Vorgang mit Ihrem eigenen *`detector ID`* aus. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster in Ihrem Konto.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Detektor-ID verwenden. Um die `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, besuchen Sie die Einstellungsseite in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. Das folgende Beispiel aktiviert sowohl `EKS_RUNTIME_MONITORING` als auch `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] }]'` **Note** Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind. Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Alle EKS-Cluster überwachen, jedoch einige davon ausschließen (mithilfe des Ausschluss-Tags)	1. Fügen Sie dem EKS-Cluster, den Sie von der Überwachung ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar ist `GuardDuty Managed -false`. Weitere Informationen zum Hinzufügen eines Tags finden Sie unter Arbeiten mit Tags mithilfe der CLI, API oder eksctl im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2:CreateTags* durch `eks:TagResource`. • Ersetzen Sie *ec2:DeleteTags* durch `eks:UntagResource`. • Ersetzen *access-project* durch `GuardDuty Managed` • *123456789012* Ersetzen Sie durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	3. **Note** Fügen Sie Ihrem EKS-Cluster immer das Ausschluss-Tag hinzu, bevor Sie den Wert `STATUS` von `EKS_RUNTIME_MONITORING` auf setzen. `ENABLED` Andernfalls wird der GuardDuty Security Agent auf allen EKS-Clusternin Ihrem Konto bereitgestellt. Um EKS Runtime Monitoring selektiv für Ihre Mitgliedskonten zu aktivieren, führen Sie den updateMemberDetectors API-Vorgang mit Ihrem eigenen *`detector ID`* aus. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster, die nicht von der Überwachung ausgeschlossen wurden. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Detektor-ID verwenden. Um die `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, besuchen Sie die Einstellungsseite in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. Das folgende Beispiel aktiviert sowohl `EKS_RUNTIME_MONITORING` als auch `EKS_ADDON_MANAGEMENT` :

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte

```
aws guardduty update-member-detectors --
detector-id  12abc34d567e8fa901bc2d34e56
789f0  --account-ids  111122223333  --feature
s '[{"Name" : "EKS_RUNTIME_MONITORING",
 "Status" : "ENABLED", "AdditionalConfigu
ration" : [{"Name" : "EKS_ADDON_MANAGEMENT",
 "Status" : "ENABLED"}] }]'
```

> **Note**
>
> Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Ausgewählte EKS-Cluster überwachen (mithilfe des Einschließen-Tags)	1. Fügen Sie dem EKS-Cluster ein Tag hinzu, das Sie in die Überwachung einbeziehen möchten. Das Schlüssel-Wert-Paar ist `GuardDutyManaged -true`. Weitere Informationen zum Hinzufügen eines Tags finden Sie unter Arbeiten mit Tags mithilfe der CLI, API oder eksctl im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2:CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2:DeleteTags* durch `eks:UntagResource` . • Ersetzen *access-project* durch `GuardDutyManaged` • *123456789012* Ersetzen Sie durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Um EKS Runtime Monitoring selektiv für Ihre Mitgliedskonten zu aktivieren, führen Sie den updateMem

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	berDetectors API-Vorgang mit Ihrem eigenen *detector ID* aus. Stellen Sie den Status für EKS_ADDON_MANAGEMENT als DISABLED ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster, die mit dem true Paar GuardDutyManaged — markiert wurden. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Detektor-ID verwenden. Um die detectorId für Ihr Konto und Ihre aktuelle Region zu finden, besuchen Sie die Einstellungsseite in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. Das folgende Beispiel aktiviert EKS_RUNTIME_MONITORING und deaktiviert EKS_ADDON_MANAGEMENT : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "DISABLED"}] }]'` **Note** Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Den Sicherheitsagent manuell verwalten	1. Um EKS Runtime Monitoring für Ihre Mitgliedskonten selektiv zu aktivieren, führen Sie den updateMemberDetectors API-Vorgang mit Ihrem eigenen *detector ID* aus. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Detektor-ID verwenden. Um die `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, besuchen Sie die Einstellungsseite in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITORING` und deaktiviert `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "DISABLED"}] } ]'` 2. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Sicherheitsagenten für den Amazon EKS-Cluster.

Konfiguration von EKS Runtime Monitoring für ein eigenständiges Konto (API)

Ein eigenständiges Konto besitzt die Entscheidung, ob ein Schutzplan AWS-Konto in einem bestimmten Bereich aktiviert oder deaktiviert werden soll AWS-Region.

Wenn Ihr Konto durch oder durch AWS Organizations die Einladungsmethode mit einem GuardDuty Administratorkonto verknüpft ist, gilt dieser Abschnitt nicht für Ihr Konto. Weitere Informationen finden Sie unter Konfiguration von EKS Runtime Monitoring für Umgebungen mit mehreren Konten (API).

Nachdem Sie Runtime Monitoring aktiviert haben, stellen Sie sicher, dass der GuardDuty Security Agent durch automatische Konfiguration oder manuelle Bereitstellung installiert wird. Stellen Sie sicher, dass Sie den Security Agent installieren, um alle im folgenden Verfahren aufgeführten Schritte abzuschließen.

Auf der Grundlage von Ansätze zur Verwaltung von GuardDuty Sicherheitsagenten in Amazon EKS-Clustern können Sie einen bevorzugten Ansatz wählen und die in der folgenden Tabelle aufgeführten Schritte ausführen.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Verwalten Sie den Security Agent über GuardDuty (Überwachen Sie alle EKS-Cluster)	1. Führen Sie die updateDetector-API aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den `features`-Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als `ENABLED` übergeben. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster in Ihrem Konto. 2. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Detektor-ID verwenden. Um die `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, besuchen Sie die Einstellungsseite

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. Das folgende Beispiel aktiviert sowohl `EKS_RUNTIME_MONITORING` als auch `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] }]'`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Alle EKS-Cluster überwachen, jedoch einige davon ausschließen (mithilfe des Ausschluss-Tags)	1. Fügen Sie dem EKS-Cluster, den Sie von der Überwachung ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar ist `GuardDuty Managed -false`. Weitere Informationen zum Hinzufügen eines Tags finden Sie unter Arbeiten mit Tags mithilfe der CLI, API oder eksctl im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2:CreateTags* durch `eks:TagResource`. • Ersetzen Sie *ec2:DeleteTags* durch `eks:UntagResource`. • Ersetzen *access-project* durch `GuardDuty Managed` • *123456789012* Ersetzen Sie durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	3. **Note** Fügen Sie Ihrem EKS-Cluster immer das Ausschluss-Tag hinzu, bevor Sie den Wert `STATUS` von `EKS_RUNTIME_MONITORING` auf setzen. `ENABLED` Andernfalls wird der GuardDuty Security Agent auf allen EKS-Clusts in Ihrem Konto bereitgestellt. Führen Sie die updateDetector-API aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den `features`-Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als `ENABLED` übergeben. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster, die nicht von der Überwachung ausgeschlossen wurden. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Detektor-ID verwenden. Um die `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, besuchen Sie die Einstellungsseite in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. Das folgende Beispiel aktiviert sowohl `EKS_RUNTIME_MONITORING` als auch `EKS_ADDON_MANAGEMENT` :

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	`aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] }]'`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Ausgewählte EKS-Cluster überwachen (mithilfe des Einschließen-Tags)	1. Fügen Sie dem EKS-Cluster ein Tag hinzu, das Sie in die Überwachung einbeziehen möchten. Das Schlüssel-Wert-Paar ist `GuardDutyManaged -true`. Weitere Informationen zum Hinzufügen eines Tags finden Sie unter Arbeiten mit Tags mithilfe der CLI, API oder eksctl im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2:CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2:DeleteTags* durch `eks:UntagResource` . • Ersetzen *access-project* durch `GuardDutyManaged` • *123456789012* Ersetzen Sie durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Führen Sie die updateDetector-API aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	`features`-Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als `ENABLED` übergeben. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster, die mit dem `true` Paar `GuardDutyManaged` — markiert wurden. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Detektor-ID verwenden. Um die `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, besuchen Sie die Einstellungsseite in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITORING` und deaktiviert `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] }]'`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Den Sicherheitsagent manuell verwalten	1. Führen Sie die updateDetector-API aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den `features`-Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als `ENABLED` übergeben. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Detektor-ID verwenden. Um die `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, besuchen Sie die Einstellungsseite in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITORING` und deaktiviert `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] }]'` 2. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Sicherheitsagenten für den Amazon EKS-Cluster.

Migrieren von EKS Runtime Monitoring zu Runtime Monitoring

Mit der Einführung von GuardDuty Runtime Monitoring wurde der Umfang der Bedrohungserkennung auf Amazon ECS-Container und Amazon EC2-Instances ausgeweitet. Die Erfahrung mit EKS Runtime Monitoring wurde nun in Runtime Monitoring zusammengefasst. Sie können Runtime

Monitoring aktivieren und einzelne GuardDuty Sicherheitsagenten für jeden Ressourcentyp (Amazon EC2-Instance, Amazon ECS-Cluster und Amazon EKS-Cluster) verwalten, für den Sie das Laufzeitverhalten überwachen möchten.

GuardDuty hat die Konsolenerfahrung für EKS Runtime Monitoring in Runtime Monitoring konsolidiert. GuardDuty empfiehlt Überprüfen Sie den Konfigurationsstatus von EKS Runtime Monitoring undMigrieren von EKS Runtime Monitoring zu Runtime Monitoring.

Stellen Sie im Rahmen der Migration zu Runtime Monitoring sicher, dass Deaktivieren Sie EKS Runtime Monitoring Dies ist wichtig, denn wenn Sie sich später dafür entscheiden, Runtime Monitoring zu deaktivieren und EKS Runtime Monitoring nicht zu deaktivieren, fallen weiterhin Nutzungskosten für EKS Runtime Monitoring an.

Um von EKS Runtime Monitoring zu Runtime Monitoring zu migrieren

1. Die GuardDuty Konsole unterstützt EKS Runtime Monitoring als Teil von Runtime Monitoring.

   Sie können mit der Verwendung von Runtime Monitoring Überprüfen Sie den Konfigurationsstatus von EKS Runtime Monitoring von Ihrer Organisation und Ihren Konten aus beginnen.

   Stellen Sie sicher, dass Sie EKS Runtime Monitoring nicht deaktivieren, bevor Sie Runtime Monitoring aktivieren. Wenn Sie EKS Runtime Monitoring deaktivieren, wird auch die Amazon EKS-Zusatzverwaltung deaktiviert. Fahren Sie mit den folgenden Schritten in der angegebenen Reihenfolge fort.
2. Stellen Sie sicher, dass Sie alle erfüllenVoraussetzungen für die Aktivierung von Runtime Monitoring.
3. Aktivieren Sie die Laufzeit-Überwachung, indem Sie die gleichen Einstellungen der Organisationskonfiguration für die Laufzeit-überwachung replizieren wie für die EKS-Laufzeit-Überwachung. Weitere Informationen finden Sie unter Laufzeitüberwachung aktivieren.
   - Wenn Sie ein eigenständiges Konto haben, müssen Sie Runtime Monitoring aktivieren.

     Wenn Ihr GuardDuty Security Agent bereits installiert ist, werden die entsprechenden Einstellungen automatisch repliziert und Sie müssen die Einstellungen nicht erneut konfigurieren.
   - Wenn Sie eine Organisation mit Einstellungen für die automatische Aktivierung haben, stellen Sie sicher, dass Sie dieselben Einstellungen für die automatische Aktivierung für Runtime Monitoring replizieren.

- Wenn Sie eine Organisation haben, deren Einstellungen für bestehende aktive Mitgliedskonten einzeln konfiguriert sind, stellen Sie sicher, dass Sie Runtime Monitoring aktivieren und den GuardDuty Security Agent für diese Mitglieder individuell konfigurieren.

4. Nachdem Sie sichergestellt haben, dass die Einstellungen für Runtime Monitoring und GuardDuty Security Agent korrekt sind, deaktivieren Sie EKS Runtime Monitoring, indem Sie entweder die API oder den AWS CLI Befehl verwenden.
5. (Optional) Wenn Sie alle mit dem GuardDuty Security Agent verknüpften Ressourcen bereinigen möchten, finden Sie weitere Informationen unterDeaktivieren, Deinstallieren und Bereinigen von Ressourcen in Runtime Monitoring.

Wenn Sie EKS Runtime Monitoring weiterhin verwenden möchten, ohne Runtime Monitoring zu aktivieren, finden Sie weitere Informationen unterEKS-Laufzeitüberwachung in GuardDuty. Wählen Sie je nach Anwendungsfall die Schritte aus, um EKS Runtime Monitoring für ein eigenständiges Konto oder für mehrere Mitgliedskonten zu konfigurieren.

Überprüfen Sie den Konfigurationsstatus von EKS Runtime Monitoring

Verwenden Sie die folgenden APIs oder AWS CLI Befehle, um den vorhandenen Konfigurationsstatus von EKS Runtime Monitoring zu überprüfen.

Um den vorhandenen EKS Runtime Monitoring-Konfigurationsstatus in Ihrem Konto zu überprüfen

- Führen Sie aus GetDetector, um den Konfigurationsstatus Ihres eigenen Kontos zu überprüfen.
- Alternativ können Sie den folgenden Befehl ausführen, indem Sie Folgendes verwenden AWS CLI:

```
aws guardduty get-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
region us-east-1
```

Stellen Sie sicher, dass Sie die Detektor-ID Ihrer AWS-Konto und der aktuellen Region ersetzen. Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

Um den bestehenden EKS Runtime Monitoring-Konfigurationsstatus für Ihr Unternehmen zu überprüfen (nur als delegiertes GuardDuty Administratorkonto)

- Führen Sie aus DescribeOrganizationConfiguration, um den Konfigurationsstatus Ihrer Organisation zu überprüfen.

  Alternativ können Sie den folgenden Befehl ausführen mit AWS CLI:

  ```
  aws guardduty describe-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1
  ```

  Stellen Sie sicher, dass Sie die Detektor-ID durch die Detektor-ID Ihres delegierten GuardDuty Administratorkontos und die Region durch Ihre aktuelle Region ersetzen. Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

Deaktivierung von EKS Runtime Monitoring nach der Migration zu Runtime Monitoring

Nachdem Sie sichergestellt haben, dass die vorhandenen Einstellungen für Ihr Konto oder Ihre Organisation in Runtime Monitoring repliziert wurden, können Sie EKS Runtime Monitoring deaktivieren.

Um EKS Runtime Monitoring zu deaktivieren

- Um EKS Runtime Monitoring in Ihrem eigenen Konto zu deaktivieren

  Führen Sie die UpdateDetector API mit Ihrer eigenen Region aus*detector-id*.

  Alternativ können Sie den folgenden AWS CLI Befehl verwenden. Ersetze es *12abc34d567e8fa901bc2d34e56789f0* durch deine eigene Region*detector-id*.

  ```
  aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
  features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "DISABLED"}]'
  ```

- Um EKS Runtime Monitoring für Mitgliedskonten in Ihrer Organisation zu deaktivieren

  Führen Sie die UpdateMemberDetectors API mit der Region *detector-id* des delegierten GuardDuty Administratorkontos der Organisation aus.

Alternativ können Sie den folgenden AWS CLI Befehl verwenden. *12abc34d567e8fa901bc2d34e56789f0*Ersetzen Sie durch die Region *detector-id* des delegierten GuardDuty Administratorkontos der Organisation und *111122223333* durch die AWS-Konto ID des Mitgliedskontos, für das Sie diese Funktion deaktivieren möchten.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING",
 "Status" : "DISABLED"}]'
```

- So aktualisieren Sie die Einstellungen für die automatische Aktivierung von EKS Runtime Monitoring für Ihre Organisation

  Führen Sie den folgenden Schritt nur aus, wenn Sie die Einstellungen für die automatische Aktivierung von EKS Runtime Monitoring entweder für neue (NEW) oder alle (ALL) Mitgliedskonten in der Organisation konfiguriert haben. Wenn Sie es bereits als konfiguriert habenNONE, können Sie diesen Schritt überspringen.

  > **Note**
  >
  > Wenn Sie die Konfiguration für die automatische Aktivierung von EKS Runtime NONE Monitoring auf auf einstellen, wird EKS Runtime Monitoring nicht automatisch für ein vorhandenes Mitgliedskonto aktiviert oder wenn ein neues Mitgliedskonto Ihrer Organisation beitritt.

  Führen Sie die UpdateOrganizationConfiguration API mit der Region *detector-id* des delegierten GuardDuty Administratorkontos der Organisation aus.

  Alternativ können Sie den folgenden AWS CLI Befehl verwenden. *12abc34d567e8fa901bc2d34e56789f0*Ersetzen Sie durch die Region *detector-id* des delegierten GuardDuty Administratorkontos der Organisation. Ersetzen Sie das *EXISTING_VALUE* durch Ihre aktuelle Konfiguration für die automatische GuardDuty Aktivierung.

  ```
  aws guardduty update-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members EXISTING_VALUE
   --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NONE"}]'
  ```

GuardDuty Release-Versionen des Security Agents

GuardDuty veröffentlicht von Zeit zu Zeit eine aktualisierte Agentenversion. Wenn den Agenten automatisch GuardDuty verwaltet, GuardDuty ist so konzipiert, dass er den Agenten in Ihrem Namen aktualisiert. Wenn Sie den Agenten manuell verwalten, sind Sie dafür verantwortlich, die Agentenversion für Ihre Ressourcentypen — Amazon EC2-Instances, Amazon ECS-Cluster und Amazon EKS-Cluster — zu aktualisieren.

In den folgenden Abschnitten finden Sie die Versionsversionen der GuardDuty Security Agents und die zugehörigen Versionshinweise für alle unterstützten Ressourcentypen.

Topics

- GuardDuty Security Agent-Versionen für Amazon EC2-Instances
- GuardDuty Versionen der Sicherheitsagenten für Amazon ECS-EC2 Bottlerocket
- GuardDuty Security Agent-Versionen für AWS Fargate (Nur Amazon ECS)
- GuardDuty Security Agent-Versionen für Amazon EKS-Ressourcen
- Zusätzliche Ressourcen — nächste Schritte

GuardDuty Security Agent-Versionen für Amazon EC2-Instances

Die folgende Tabelle zeigt den Versionsverlauf für den GuardDuty Security Agent für Amazon EC2.

Version des SSM-Vertriebspartners	Agent-Version	Versionshinweise	Datum der Verfügbarkeit
v1.16.0	v1.16.0	Unterstützung für Kernel 6.19, 7.0, 7.1 hinzugefügt. Unterstützung für Ubuntu 26.04, Debian 13, RedHat 10.2, CentOS Stream 10, Rocky Linux 10.1, Fedora 43 und Fedora 44 hinzugefügt. Eine	17. Juli 2026

Version des SSM-Vertriebspartners	Agent-Version	Versionshinweise	Datum der Verfügbarkeit
		Liste aller verifizierten Betriebssystemvertreilungen für Amazon EC2-Ressourcen finden Sie unter. Überprüfen Sie die architektonischen Anforderungen Allgemeine Aktualisierungen der Sicherheitsfunktionen.	
v1.15.0	v1.15.0	Neue Agentenfunktionen zur Unterstützung einer optimierten Ereigniserfassung, ermöglichen eine schnellere Filterbereitstellung und eine verbesserte Erkennungsgeschwindigkeit. Allgemeine Aktualisierungen der Sicherheitsfunktionen.	14. Mai 2026

Version des SSM-Vertriebspartners	Agent-Version	Versionshinweise	Datum der Verfügbarkeit
v1.9.2	v1.9.2	Unterstützung für Kernel 6.15, 6.16, 6.17, 6.18 hinzugefügt. Unterstützung für Alma Linux 9, Alma Linux 10 und SUSE Linux Enterprise Server 16 hinzugefügt. Eine Liste aller verifizierten Betriebssystemverteilungen für Amazon EC2-Ressourcen finden Sie unter. Überprüfen Sie die architektonischen Anforderungen	24. Februar 2026
v1.9.1	v1.9.1	Allgemeine Leistungsoptimierung und Aktualisierungen der Sicherheitsfunktionen.	10. November 2025
v1.9.0	v1.9.0	Allgemeine Leistungsoptimierung und Verbesserungen.	23. Oktober 2025
v1.8.0	v1.8.0	Allgemeine Leistungsoptimierung und Verbesserungen.	12. August 2025

Version des SSM-Vertriebspartners	Agent-Version	Versionshinweise	Datum der Verfügbarkeit
v1.7.2	v1.7.1	Verbesserte Unterstützung für die lokale Agenteninstallation für RPM-basierte Linux-Distributionen.	23. Juli 2025
v1.7.1	1.7.1	Unterstützung für Fedora 40 und Fedora 41 hinzugefügt. Eine Liste aller verifizierten Betriebssystemverteilungen für Amazon EC2-Ressourcen finden Sie unter. Überprüfen Sie die architektonischen Anforderungen Allgemeine Leistungsoptimierung und Verbesserungen.	03. Juni 2025

Version des SSM-Vertriebspartners	Agent-Version	Versionshinweise	Datum der Verfügbarkeit
v1.7.0	v1.7.0	Unterstützung für Oracle Linux-Versionen 8.9 und 9.3 sowie Rocky Linux Version 9.5 hinzugefügt. Eine Liste aller verifizierten Betriebssystemverteilungen für Amazon EC2-Ressourcen finden Sie unter. Überprüfen Sie die architektonischen Anforderungen Die Auflösung der Container-ID wurde verbessert. Allgemeine Leistungsoptimierung und Verbesserungen.	03. April 2025
v1.6.0	v1.6.0	Allgemeine Leistungsoptimierung und Verbesserungen.	6. Februar 2025

Version des SSM-Vertriebspartners	Agent-Version	Versionshinweise	Datum der Verfügbarkeit
v1.5.0	v1.5.0	Unterstützung für CentOS Stream 9.0, RedHat 9.4, Fedora 34.0 und Ubuntu 24.04 hinzugefügt. Unterstützung für ARM-Instanzen für Ergebnisse. `.../MetadataDNSRebind` Allgemeine Leistungsoptimierung und Verbesserungen.	20. November 2024
v1.3.1	v1.3.1	Unterstützung für benutzerdefinierte DNS-Resolver.	12. September 2024
v1.3.0	v1.3.0	Allgemeine Leistungsoptimierung und Verbesserungen. Beinhaltet Unterstützung für die Erfassung zusätzlicher Sicherheitssignale für die ZukunftGuardDuty Findetypen für die Laufzeitüberwachung.	19. August 2024

Version des SSM-Vertriebspartners	Agent-Version	Versionshinweise	Datum der Verfügbarkeit
v1.2.0	v1.2.0	Unterstützt die Betriebssystem-Distributionen Ubuntu 20.04, Ubuntu 22.04, Debian 11 und Debian 12. Unterstützt Kernel 6.5 und 6.8. Allgemeine Leistungsoptimierung und Verbesserungen.	13. Juni 2024
v1.1.0	v1.1.0	Unterstützt die GuardDuty automatische Agentenkonfiguration in Runtime Monitoring für Amazon EC2-Instances. Unterstützt neue Sicherheitssignale und Erkenntnisse, die mit der Ankündigung der allgemeinen Verfügbarkeit von Runtime Monitoring für EC2-Instances veröffentlicht wurden. Allgemeine Leistungsoptimierung und Verbesserungen.	26. März 2024

Version des SSM-Vertriebspartners	Agent-Version	Versionshinweise	Datum der Verfügbarkeit
v1.0.2	v1.0.2	Unterstützt die neuesten Amazon ECS-AMIs.	2. Februar 2024
v1.0.1	v1.0.1	Agentenversionen, die vor Version 1.0.2 veröffentlicht wurden, sind nicht mit Amazon ECS-AMIs kompatibel, die nach dem 31. Januar 2024 eingeführt wurden. Allgemeine Leistungsoptimierung und Verbesserungen.	23. Januar 2024
v1.0.0	v1.0.0	Erste Veröffentlichung der RPM-Installation. Agentenversionen, die vor Version 1.0.2 veröffentlicht wurden, sind nicht kompatibel mit Amazon ECS-AMIs, die nach dem 31. Januar 2024 eingeführt wurden.	26. November 2023

GuardDuty Versionen der Sicherheitsagenten für Amazon ECS-EC2 Bottlerocket

Die folgende Tabelle zeigt den Versionsverlauf des GuardDuty Security Agents für Amazon ECS-EC2 Bottlerocket-Instances. Der Agent läuft als Host-Container auf Bottlerocket ECS-2 und optimierter AMI-Version und ECS-3 höher. `v1.62.1`

Version für SSM-Vertriebspartner	Agent-Version	Versionshinweise	Datum der Verfügbarkeit
v1.16.0	v1.16.0	Erste Veröffentlichung des GuardDuty Sicherheitsagenten für Amazon ECS-EC2 Bottlerocket-Instances. Unterstützt Bottlerocket ECS-2 und ECS-3 Varianten (x86_64 und aarch64).	17. Juli 2026

GuardDuty Security Agent-Versionen für AWS Fargate (Nur Amazon ECS)

Die folgende Tabelle zeigt den Versionsverlauf für den GuardDuty Security Agent für Fargate (nur Amazon ECS).

Agent-Version	Container-Bild	Versionshinweise	Datum der Verfügbarkeit
v1.16.0	x86_64 (AMD64): `sha256:711fa37e2cce0417ba3310d81439d6b11170e446f685146b36916e4e38c1560d` Graviton (ARM64): `sha256:6851e00893eee958085a`	Allgemeine Aktualisierungen der Sicherheitsfunktionen.	17. Juli 2026

Agent-Version	Container-Bild	Versionshinweise	Datum der Verfügbarkeit
	daccddf91 bdc009ebd dcd46b4da 6fb1962b1 32d47454		
v1.15.0	x86_64 (AMD64): sha256:66 446df341b ee1a1e218 aa46b7807 d0d047026 6c8f374c5 dbd97efcd b8356348 Graviton (ARM64): sha256:b0 def2aa8ca b6b2060c7 03f386fdb 29dc41660 54e0509a9 362b21a6e d7f9def7	Neue Agentenfunktionen zur Unterstützung einer optimierten Ereigniserfassung, ermöglichen eine schnellere Filterbereitstellung und eine verbesserte Erkennungsgeschwindigkeit. Allgemeine Aktualisierungen der Sicherheitsfunktionen.	28. Mai 2026

Agent-Version	Container-Bild	Versionshinweise	Datum der Verfügbarkeit
v1.9.0	x86_64 (AMD64): `sha256:fd9acaa2326f180f0ed0c5a25d8ff0a2d0498a6e900c34c68d4e973ea7fb26a8` Graviton (ARM64): `sha256:0b04f8c28956684e752677bfd83dbc45afc8a43f7791fa44667b8078ba48a295`	Allgemeine Leistungsoptimierung und Sicherheitsverbesserungen.	28. Oktober 2025

Agent-Version	Container-Bild	Versionshinweise	Datum der Verfügbarkeit
v1.8.0	x86_64 (AMD64): `sha256:4425417f39e38b24c1be428bacad1dad53e0645530dcf4422436353bfe358e3a` Graviton (ARM64): `sha256:aff069418fd6825846f8f575c49906a67c8a446d12d9ed0d21ab95bd0d05497b`	Allgemeine Leistungsoptimierung und Verbesserungen.	12. August 2025

Agent-Version	Container-Bild	Versionshinweise	Datum der Verfügbarkeit
v1.7.0	x86_64 (AMD64): `sha256:bf9197abdf853607e5fa392b4f97ccdd6ca56dd179be3ce8849e552d96582ac8` Graviton (ARM64): `sha256:56c8683c948bcd82c0dbcebf755204365ac7285994693c11717bd45f86e279c2`	Verbesserte Container-ID-Auflösung. Allgemeine Leistungsoptimierung und Verbesserungen.	04. April 2025

Agent-Version	Container-Bild	Versionshinweise	Datum der Verfügbarkeit
v1.6.0	x86_64 (AMD64): `sha256:c8dea71d372bc47b2f236f7a091b9a9b06bc8193c1cfe4c9346eb50f89258897` Graviton (ARM64): `sha256:f4032a566b90537646c2a987bef42eca1b498078ccc58a848603f877971a8dbe`	Allgemeine Leistungsoptimierung und Verbesserungen.	6. Februar 2025

Agent-Version	Container-Bild	Versionshinweise	Datum der Verfügbarkeit
v1.5.0	x86_64 (AMD64): `sha256:5e6fdc41f9eb748219d0498cd6c1dba6a19d875daec50167a0ac80e5028eac54` Graviton (ARM64): `sha256:d56801ff6864d601474010 3b70b1c38431851358d182613bede20fe21090e734`	Unterstützung für ARM-Aufgaben für `.../MetadataDNSRebind` Ergebnisse. Allgemeine Leistungsoptimierung und Verbesserungen.	14. November 2024

Agent-Version	Container-Bild	Versionshinweise	Datum der Verfügbarkeit
v1.4.1	x86_64 (AMD64): `sha256:ef36a11151ec2d3d7db22273bfb954750dee76f0ac7bec37a7ba7e74c3de1c78` Graviton (ARM64): `sha256:a8844544a59d6b4cba98f8e528b513ac2d97432f208e3ad497cc16b331aa9faa`	Härtung des Container-Images. Allgemeine Leistungsoptimierung und Verbesserungen.	24. Oktober 2024

Agent-Version	Container-Bild	Versionshinweise	Datum der Verfügbarkeit
v1.3.1	x86_64 (AMD64): `sha256:a6e2307d796e2875907bc4c1c69622c906f3192ddc42ef27b99e0a8f0979f3e0` Graviton (ARM64): `sha256:ad1b6539d806edb504f17e6bcfb8b4026c5e822300afc31c0d23c6a08f9b99e9`	Unterstützung für benutzerdefinierte DNS-Resolver.	11. September 2024

Agent-Version	Container-Bild	Versionshinweise	Datum der Verfügbarkeit

v1.3.0	x86_64 (AMD64):
	`sha256:f1ad3fb2dc55a1110c60eecf4453b9f9c02f29acb261df39814e7d29296bf831`
	
	Graviton (ARM64):
	`sha256:ff81a755d46681e409f55a95beedae9ebbcf5336e1c0b1e6348af7c6518bdbb1`
		Allgemeine Leistungsoptimierung und Verbesserungen.
		
		Beinhaltet Unterstützung für die Erfassung zusätzlicher Sicherheitssignale für die Zukunft GuardDuty GuardDuty Findetypen für die Laufzeitüberwachung.
			9. August 2024

Agent-Version	Container-Bild	Versionshinweise	Datum der Verfügbarkeit

v1.2.0	x86_64 (AMD64):
	`sha256:1dbad20ac2dc66d52d00bb28dde4281fe0d3c5f261b1649b247c2369d9e26b93`
	
	Graviton (ARM64):
	`sha256:91930f8446f5f95b93b8ccb18773992affa401eb3f42da89d68077a56bafa6cd`
		Allgemeine Leistungsoptimierung und Verbesserungen.	31. Mai 2024

Agent-Version	Container-Bild	Versionshinweise	Datum der Verfügbarkeit
v1.1.0	x86_64 (AMD64): `sha256:83ce3cf2ef85a349ed1797a8cf30a008ac5d8c9f673f2835823957e9dcf71657` Graviton (ARM64): `sha256:0d4b61648d7bdeab8ab8d94684f805498927c7d437d318204dcccfe8c9383dc7`	Unterstützt neue Sicherheitssignale und Erkenntnisse. Allgemeine Leistungsoptimierung und Verbesserungen.	01. Mai 2024

Agent-Version	Container-Bild	Versionshinweise	Datum der Verfügbarkeit

v1.0.1	x86_64 (AMD64):
	`sha256:9f8cd438fb66f62d09bfc641286439f7ed5177988a314a6021ef4ff880642e68`
	
	Graviton (ARM64):
	`sha256:82c66bb615bd0d1e96db77b1f1fb51dc03220caa593b1962249571bf7147d1b7`
		Allgemeine Leistungsoptimierung und Verbesserungen.	26. Januar 2024

Agent-Version	Container-Bild	Versionshinweise	Datum der Verfügbarkeit
v1.0.0	x86_64 (AMD64): `sha256:359b8b014e5076c625daa1056090e522631587a7afa3b2e055edda6bd1141017` Graviton (ARM64): `sha256:b9438690fa8a86067180a11658bec0f4f838ae3fbd225d04b9306250648b3984`	Erste Veröffentlichung des GuardDuty Security Agents für AWS Fargate (nur Amazon ECS).	26. November 2023

GuardDuty Security Agent-Versionen für Amazon EKS-Ressourcen

GuardDuty veröffentlicht von Zeit zu Zeit eine aktualisierte Agentenversion. Wenn der Agent automatisch GuardDuty verwaltet wird, ist er so konzipiert, dass er die Agenten-Updates in Ihrem Namen verwaltet. Wenn Sie den Agenten manuell verwalten, sind Sie dafür verantwortlich, die Agentenversion für Ihre Amazon EKS-Cluster zu aktualisieren.

Bevor Sie den Agenten auf eine bestimmte Version aktualisieren, fügen Sie die Image-Registrierung für GuardDuty zu Ihrem Admission Controller hinzu. `allowed-container-registries` Weitere Informationen finden Sie unter Amazon ECR-Repository-Hosting-Agent GuardDuty.

Die folgende Tabelle zeigt den Versionsverlauf des Amazon GuardDuty EKS-Add-On-Agenten.

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende der Standardunterstützung [1]
v1.16.0	x86_64 (AMD64): `sha256:8a4ef4b5b5e6fce0a4b5a13922e65179293ee15a8812a2c7678b1c4b31e1f305` Graviton (ARM64): `sha256:0a73c1d905a39db94f6ea37d98784dac84961e9199935fae20345de7aa3a57b7`	Unterstützung für Kernel 6.19, 7.0, 7.1 hinzugefügt. Allgemeine Aktualisierungen der Sicherheitsfunktionen.	17. Juli 2026	–
v1.15.0	x86_64 (AMD64): `sha256:512642a5f9d9a316aa9100368acfdbae2481be7a5cfe9929571c1bb6e19c66fe`	Neue Agentenfunktionen zur Unterstützung einer optimierten Ereigniserfassung, ermöglichen eine schnellere Filterbereitstellung und eine	14. Mai 2026	–

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende der Standardunterstützung [1]
	Graviton (ARM64): `sha256:f017e755615ae999fe5f163886f681508e8f53feea7e64e7ada733cdedb368d8`	verbesserte Erkennungsgeschwindigkeit. Allgemeine Aktualisierungen der Sicherheitsfunktionen.		
v1.12.2	x86_64 (AMD64): `sha256:06c25ab9fff7ee93048e5f34148c9627366323` `5937199b4bd2e28b5ee2e5c080` Graviton (ARM64): `sha256:f89962d971350ff6ab408cf6ec7bca9dd06152f0172b7f9c68ae770cc0fc4598`	Allgemeine Aktualisierungen der Sicherheitsfunktionen.	26. März 2026	–

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende der Standardunterstützung [1]
v1.12.1	x86_64 (AMD64): `sha256:f29a597745e5acff48809bebac7d8091bbc38229453dd26710c549b817362491` Graviton (ARM64): `sha256:089cebdc7e891177e107a099c9a4e362d9d74b5362cd374b448a16078040f6c6`	Allgemeine Leistungsoptimierung und Aktualisierungen der Sicherheitsfunktionen.	17. November 2025	–

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende der Standardunterstützung [1]
v1.11.0	x86_64 (AMD64): `sha256:7c398fd50dee5fe493c361aa7fe191e094ddfa000c65b449a9ed6a5cd53610e7` Graviton (ARM64): `sha256:98a547b47d4770f45e75eb9730c807d9265722ca2f391e0aa5cb19e487ab455f`	Unterstützung für die Betriebssystem-Distributionen Fedora 40 und Fedora 4.1 wurde hinzugefügt. Weitere Informationen finden Sie unter Validierung der architektonischen Anforderungen (für EKS). Allgemeine Leistungsoptimierung und Sicherheitsverbesserungen.	29. August 2025	–

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende der Standardunterstützung [1]
v1.10.0	x86_64 (AMD64): `sha256:6dcbe5b055e1ef0af903071ede0b08f755ad5b7e9774a67df5399efdaa1f3d7d` Graviton (ARM64): `sha256:f0536882268 9610a4bab543abf93d3e070b1b559e62a2e67d82dfa9837600f72`	Die Auflösung der Container-ID wurde verbessert. Allgemeine Leistungsoptimierung und Verbesserungen.	04. April 2025	–

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende der Standardunterstützung [1]
v1.9.0	x86_64 (AMD64): `sha256:51c5789ef6570f9bec879ac48a8f4769718cbc31e45430032569917e219af63f` Graviton (ARM64): `sha256:9c2f74e7ea0827b7e422ae4c91fffc6c2bc41a1cdb96c7191d05259d337154e1`	Allgemeine Leistungsoptimierung und Verbesserungen.	02. März 2025	–

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende der Standardunterstützung [1]
v1.8.1	x86_64 (AMD64): `sha256:f2ce8cf89dbe17e3388cecb35053544dadf21af7770545f8d4b50384076aff47` Graviton (ARM64): `sha256:30f586e4b694e704bcafadfa9081ab0aeff3cfbcde39743a0f1e24f77d79627f`	Unterstützung für CentOS Stream 9.0, RedHat 9.4, Fedora 34.0 und Ubuntu 24.04 hinzugefügt. Unterstützung für ARM-Instanzen zum Auffinden `.../MetadataDNSRebind` Allgemeine Leistungsoptimierung und Verbesserungen.	23. November 2024	–

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende der Standardunterstützung [1]

v1.7.1	x86_64 (AMD64): `sha256:b8b86b5d0872c8b67fecf64ec3d17266636054`
	`5435a1752447d510951a7fd749`
	
	Graviton (ARM64): `sha256:40ac4cfc354fd430ba7897ca1632e`
	`9a500ed13eeb0c315c5bcad38680e76b6e9`
		Allgemeine Leistungsoptimierung und Verbesserungen.
		
		Beinhaltet Unterstützung für die Erfassung zusätzlicher Sicherheitssignale für die Zukunft GuardDuty Findetypen für die Laufzeitüberwachung.
		
		Unterstützung für benutzerdefinierte DNS-Resolver.
			13. September 2024	–

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende der Standardunterstützung [1]
v1.7.0	x86_64 (AMD64): `sha256:f3a2a8806e6c2a7fd63a91cccf6f7dffcd7e68554a423d610cea8c7e8f2185ec` Graviton (ARM64): `sha256:b1a6db35a072c0de3c695e5e909a03e6c4e1fdbe47ecfaeb2784435cf67ebe0a`	Allgemeine Leistungsoptimierung und Verbesserungen. Beinhaltet Unterstützung für die Erfassung zusätzlicher Sicherheitssignale für die ZukunftGuardDuty Findetypen für die Laufzeitüberwachung.	17. August 2024	–

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende der Standardunterstützung [1]
v1.6.1	x86_64 (AMD64): `sha256:30650708a6601f6d6b9046f54b30f5fd65af296b1e40b8c24426b9bdb07c3ab1` Graviton (ARM64): `sha256:5f637c42ffb306b20f776d9d83e1e0b4be40ce245be44afcf43a8902b4d71019`	Allgemeine Leistungsoptimierung und Verbesserungen.	14. Mai 2024	–

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende der Standardunterstützung [1]
v1.6.0	x86_64 (AMD64): `sha256:7dabcbee30d8b053676752fbc19e89f77272d9a6a53cc93731f5872180ef9010` Graviton (ARM64): `sha256:9710f53afccdf4f22b265a1a6fc27f1469403af1f7d5d08c4869a7269cdd2650`	• Unterstützt die GuardDuty automatische Agentenkonfiguration für EKS/EC2 Ressourcen. • Unterstützt die neuen Sicherheitssignale und Erkenntnisse. Weitere Informationen erhalten Sie unter Gesammelte Runtime-Ereignistypen, die GuardDuty verwendet und GuardDuty Findetypen für die Laufzeitüberwachung. • Allgemeine Leistungsoptimierung und Verbesserungen.	29. April 2024	–

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende der Standardunterstützung [1]
v1.5.0	x86_64 (AMD64): `sha256:e09a4e70af4058a212f172cc8eb3fc23ad9bed547ed609faa2bb82cf7cc5532d` Graviton (ARM64): `sha256:afc9a3f8f17ae12499d76069efcf1b46271a5a4b2b3f6ba5de54637b8f55d5c6`	• Allgemeine Leistungsoptimierung und Verbesserungen. • Sicherheitsverbesserungen, einschließlich neuer Ereignistypen, finden Sie unter Gesammelte Laufzeit-Ereignistypen. • Leistungsverbesserungen im Zusammenhang mit der CPU-Auslastung.	07. März 2024	–

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende der Standardunterstützung [1]
v1.4.1	x86_64 (AMD64): `sha256:66d491927763742660faa87cc2c39bb97b7873039157ae8b90bc999cb73d0b9c` Graviton (ARM64): `sha256:537a330b2dd82357024fb6daeb8761034b7defd43b10dffe0792c9e6d0778b40`	Allgemeine Leistungsoptimierung und Verbesserungen.	16. Januar 2024	–

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende der Standardunterstützung [1]
v1.4.0	x86_64 (AMD64): `sha256:848ce13d9430bad554ac23d4699551505326ada2a88e1a721fe9f86b56b52c0f` Graviton (ARM64): `sha256:0c650aeafeeb5f2bcb8b989ac849bedc1fae1a4de1cf6306ffdd9c6aebe67f8e`	Der Manifest Mount Point unterstützt eine bessere Datenerfassung AppArmor Konfiguration im Manifest Sammle das Befehlszeilenargument Allgemeine Leistungsoptimierung und Verbesserungen	21. Dezember 202	–

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende der Standardunterstützung [1]
v1.3.1	x86_64 (AMD64): `sha256:555578fcb7b73097ade5c8404390ef16cf76a7b568490abaae01ac75992b3ea29` Graviton (ARM64): `sha256:e3ce8d66ac2121f8d476eb58f8bc50ab51336647615eb7cf514c21421cb818fd`	Wichtige Sicherheitspatches und Updates.	23. Oktober 2023	–

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende der Standardunterstützung [1]
v1.3.0	x86_64 (AMD64): `sha256:6dace2337dfbb7609811be89fb4b23ae0b865f1027ad78fbe69530bfbd46c694` Graviton (ARM64): `sha256:4928a7c6ef40e77c8ec95841323bb9a110db31f12c0ee7ab965e08b43efd01bb`	Unterstützt die Ubuntu-Plattform Unterstützt Kubernetes-Version 1.28 Allgemeine Leistungsverbesserungen und Stabilitätsverbesserungen.	5. Oktober 2023	–

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende der Standardunterstützung [1]
v1.2.0	x86_64 (AMD64): `sha256:d610413d662ec042057f05d6942496d7f2c08e9f5a077ea307ffdb5d3f11bcc3` Graviton (ARM64): `sha256:174d7ab28b2f95e5309da80d95b88ad26f602dfe72c2b351a0ef9297a1412bfa`	Zusätzlich zu AMD64-basierten Instanzen unterstützt v1.2.0 jetzt auch ARM64-basierten Instanzen. Unterstützung für Bottlerocket hinzugefügt und verifiziert Unterstützt Kubernetes-Version 1.27 Allgemeine Leistungsverbesserungen und Stabilitätsverbesserungen.	16. Juni 2023	–

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende der Standardunterstützung [1]
v1.1.0	`sha256:b19ba3a3c1a508d153263ae2fda891a7928b5ca9b3a5692db6c101829303281c`	Über Kubernetes-Versionen, die vom Security Agent unterstützt werden GuardDuty hinaus unterstützt diese Agentenversion auch Kubernetes Version 1.26. Allgemeine Leistungsverbesserungen und Stabilitätsverbesserungen.	2. Mai 2023	14. Mai 2024
v1.0.0	`sha256:e38bdd2b1323e89113f1a31bd4bc8e5a8098525dd98e6981a28b9906b1e4411e`	Erste Version des Amazon-EKS-Add-On-Agenten.	30. März 2023	14. Mai 2024

1 Informationen zur Aktualisierung Ihrer aktuellen Agentenversion, die sich dem Ende des Standardsupports nähert, finden Sie unterManuelles Aktualisieren des Security Agents für Amazon EKS-Ressourcen.

Zusätzliche Ressourcen — nächste Schritte

Weitere Informationen zu den nächsten Schritten finden Sie in den folgenden Themen:

- Voraussetzungen für die Aktivierung von Runtime Monitoring— Bei neuen Agentenversionen wird möglicherweise der Abschnitt mit den Voraussetzungen aktualisiert. Stellen Sie sicher, dass Ihre Ressourcen die neuesten Voraussetzungen erfüllen.
- Verwaltung der GuardDuty Sicherheitsagenten- Wenn Sie den Agenten manuell verwalten, sind Sie für die Verwaltung der Updates der Agentenversion verantwortlich, die auf Ihren Ressourcen ausgeführt wird. Führen Sie je nach Ressourcentyp (Amazon EKS oder Amazon EC2-Amazon ECS) die Schritte zur Aktualisierung des Security Agents durch. Stellen Sie außerdem sicher, dass Sie Ihre VPC-Endpunktkonfiguration validieren.
- Überprüfung der Statistiken zur Laufzeitabdeckung und Behebung von Problemen- Nachdem Sie den Security Agent aktualisiert haben, können Sie die Laufzeitabdeckung Ihrer Ressource beurteilen. Wenn es ein Problem mit der Netzabdeckung gibt, folgen Sie den entsprechenden Schritten zur Problembehandlung.

Deaktivieren, Deinstallieren und Bereinigen von Ressourcen in Runtime Monitoring

Dieser Abschnitt bezieht sich darauf, AWS-Konto ob Sie Runtime Monitoring oder nur die GuardDuty automatische Agentenkonfiguration für einen Ressourcentyp deaktivieren möchten.

Deaktivierung der GuardDuty automatisierten Agentenkonfiguration

GuardDuty entfernt nicht den Security Agent, der auf Ihrer Ressource installiert ist. GuardDuty Beendet jedoch die Verwaltung der Updates für den Security Agent.

GuardDuty empfängt weiterhin die Runtime-Ereignisse von Ihrem Ressourcentyp. Um Auswirkungen auf Ihre Nutzungsstatistiken zu vermeiden, sollten Sie den GuardDuty Security Agent unbedingt aus Ihrer Ressource entfernen.

Unabhängig davon, ob ein einen gemeinsam genutzten VPC-Endpunkt AWS-Konto verwendet oder GuardDuty nicht, wird der VPC-Endpunkt nicht gelöscht. Bei Bedarf müssen Sie den VPC-Endpunkt manuell löschen.

Deaktivieren von Runtime Monitoring und EKS Runtime Monitoring

Dieser Abschnitt gilt für Sie in den folgenden Szenarien:

- Sie haben EKS Runtime Monitoring nie separat aktiviert und jetzt haben Sie Runtime Monitoring deaktiviert.
- Sie deaktivieren sowohl Runtime Monitoring als auch EKS Runtime Monitoring. Wenn Sie sich über den Konfigurationsstatus von EKS Runtime Monitoring nicht sicher sind, finden Sie weitere Informationen unterÜberprüfen Sie den Konfigurationsstatus von EKS Runtime Monitoring.

  > Deaktivieren Sie Runtime Monitoring, ohne EKS Runtime Monitoring zu deaktivieren
  >
  > In diesem Szenario haben Sie irgendwann EKS Runtime Monitoring aktiviert und später auch Runtime Monitoring aktiviert, ohne EKS Runtime Monitoring zu deaktivieren. Wenn Sie Runtime Monitoring deaktivieren, müssen Sie jetzt auch EKS Runtime Monitoring deaktivieren. Andernfalls fallen weiterhin Nutzungskosten für EKS Runtime Monitoring an.

Wenn die zuvor aufgeführten Szenarien auf Sie zutreffen, GuardDuty werden in Ihrem Konto die folgenden Maßnahmen ergriffen:

- GuardDuty löscht den VPC-Endpunkt mit dem Tag`GuardDutyManaged:true`. Dies ist die VPC, die zur Verwaltung des automatisierten Sicherheitsagenten erstellt GuardDuty wurde.
- GuardDuty löscht die Sicherheitsgruppe, die als`GuardDutyManaged`: markiert wurde. `true`
- Bei einer gemeinsam genutzten VPC, die von mindestens einem Teilnehmerkonto verwendet wurde, werden GuardDuty weder der VPC-Endpunkt noch die Sicherheitsgruppe gelöscht, die der gemeinsam genutzten VPC-Ressource zugeordnet ist.
- Löscht bei einer Amazon EKS-Ressource den Security GuardDuty Agent. Dies ist unabhängig davon, ob es manuell oder über GuardDuty verwaltet wurde.

  Bei einer Amazon ECS-Ressource GuardDuty kann der Security Agent von dieser Ressource nicht deinstalliert werden, da eine ECS-Aufgabe unveränderlich ist. Dies ist unabhängig davon, wie Sie den Security Agent verwalten — manuell oder automatisch. GuardDuty Nachdem Sie Runtime Monitoring deaktiviert haben, GuardDuty hängt kein Sidecar-Container an, wenn eine neue ECS-Task ausgeführt wird. Hinweise zum Arbeiten mit Fargate-ECS Aufgaben finden Sie unter. So funktioniert Runtime Monitoring mit Fargate (nur Amazon ECS)

  Bei einer Amazon EC2-Ressource wird der Security Agent nur dann von allen vom Systems Manager (SSM) verwalteten Amazon EC2-Instances GuardDuty deinstalliert, wenn die folgenden Bedingungen erfüllt sind:

- Ihre Ressource ist nicht mit dem Tag: Exclusion gekennzeichnet. `GuardDutyManaged false`
- GuardDuty muss über Berechtigungen für den Zugriff auf die Tags in den Instanzmetadaten verfügen. Für diese EC2-Ressource ist der Zugriff auf Tags in Instance-Metadaten auf Allow gesetzt.

Wenn Sie die manuelle Verwaltung des Security Agents beenden

Unabhängig davon, welchen Ansatz Sie für die Bereitstellung und Verwaltung des GuardDuty Security Agents verwenden, müssen Sie den Security Agent entfernen, um die Überwachung der GuardDuty Laufzeitereignisse in Ihrer Ressource zu beenden. Wenn Sie die Überwachung der Laufzeitereignisse von einem Ressourcentyp in einem Konto aus beenden möchten, können Sie auch den Amazon VPC-Endpunkt löschen.

Manuelles Deinstallieren des Security Agents für Amazon EC2-Ressourcen

In diesem Abschnitt werden Methoden zur Deinstallation des GuardDuty Security Agents von Ihren Amazon EC2-Ressourcen beschrieben. Wenn Sie den Security Agent manuell verwalten, sind Sie dafür verantwortlich, den Agenten aus den Ressourcen zu entfernen. GuardDuty ergreift keine Maßnahmen in Bezug auf die von Ihnen verwalteten Ressourcen.

Wenn Sie einen Amazon VPC-Endpunkt manuell erstellt haben, können Sie nach der Deinstallation des Security Agents auf allen überwachten Ressourcentypen in Ihrem Konto wählen, ob Sie den VPC-Endpunkt löschen möchten. Dies ist ein separater Schritt. Weitere Informationen finden Sie unter To delete a VPC endpoint.

Wählen Sie je nachdem, wie Sie den Security Agent in Ihrer Ressource installiert haben, eine der folgenden Methoden, um ihn zu deinstallieren.

Themen

- Methode 1 — Mit dem Befehl Run
- Methode 2 — Mithilfe von Linux-Paketmanagern

Methode 1 — Mit dem Befehl Run

Wenn Sie den Security Agent mit installiert habenMethode 1 — Verwenden AWS Systems Manager, gehen Sie wie folgt vor, um den Agent zu deinstallieren:

Um den GuardDuty Security Agent zu deinstallieren

1. Sie können den GuardDuty Security Agent deinstallieren, indem Sie die im AWS Systems Manager Benutzerhandbuch AWS Systems Manager unter Befehl ausführen angegebenen Schritte ausführen ausführen ausführen. Verwenden Sie die Aktion Deinstallieren in den Parametern, um den GuardDuty Security Agent zu deinstallieren.

   Stellen Sie im Abschnitt Ziele sicher, dass die Auswirkung nur die Amazon EC2-Instances betrifft, von denen Sie den Security Agent deinstallieren möchten.

   Verwenden Sie das folgende GuardDuty Dokument und den folgenden Vertriebspartner:

   - Name des Dokuments: `AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`
   - Vertriebspartner: `AmazonGuardDuty-RuntimeMonitoringSsmPlugin`
2. Nachdem Sie alle Details angegeben haben und Ausführen wählen, wird der Security Agent, den es auf den Amazon EC2-Instances als Ziel eingesetzt hat, entfernt.

   Um die Amazon VPC-Endpunktkonfiguration zu entfernen, müssen Sie sowohl Runtime Monitoring als auch Amazon EKS Runtime Monitoring deaktivieren.
3. Wenn Sie auch den VPC-Endpunkt löschen möchten, der diesem Security Agent zugeordnet ist, finden Sie weitere Informationen unter. To delete a VPC endpoint

Methode 2 — Mithilfe von Linux-Paketmanagern

Wenn Sie den Security Agent mit installiert habenMethode 2: Verwenden von Linux-Paketmanagern, gehen Sie wie folgt vor, um den Agent zu deinstallieren:

Um den GuardDuty Security Agent zu deinstallieren

1. Verbinden Sie sich mit der Instance. Eine Anleitung dazu finden Sie im Amazon EC2-Benutzerhandbuch unter Herstellen einer Verbindung zu Ihrer Linux-Instance mithilfe eines SSH-Clients.
2. Befehl zur Deinstallation

   Mit dem folgenden Befehl wird der GuardDuty Security Agent von der Amazon EC2-Instance deinstalliert, mit der Sie eine Verbindung herstellen:

   - Für RPM:

```
sudo rpm -e amazon-guardduty-agent
```

- Für Debian:

```
sudo dpkg --purge amazon-guardduty-agent
```

Nachdem Sie den Befehl ausgeführt haben, können Sie auch die mit dem Befehl verknüpften Protokolle überprüfen.

3. Wenn Sie auch den VPC-Endpunkt löschen möchten, der diesem Security Agent zugeordnet ist, finden Sie weitere Informationen unterTo delete a VPC endpoint.

Der Security Agent für ECS-EC2 Bottlerocket-Ressourcen wird deinstalliert

Führen Sie die folgenden Schritte aus, um den GuardDuty Security Agent von Ihren Bottlerocket-Instances zu deinstallieren. ECS-EC2

Um den Security Agent zu deinstallieren GuardDuty

1. Um den GuardDuty Security Agent zu deinstallieren, verwenden Sie AWS Systems Manager Run Command (im AWS Systems Manager Benutzerhandbuch) und setzen Sie den Aktionsparameter auf Uninstall.

   Stellen Sie im Abschnitt Ziele sicher, dass die Auswirkung nur die Bottlerocket-Instances betrifft, von denen Sie den Security Agent deinstallieren möchten.

   Verwenden Sie das folgende GuardDuty Dokument und den folgenden Verteiler:

   - Name des Dokuments:`AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`.
   - Vertriebspartner:`AmazonGuardDuty-RuntimeMonitoringSsmPlugin`.
2. Nachdem Sie alle Details angegeben und auf Run geklickt haben, wird der Security Agent aus den Bottlerocket-Instances GuardDuty entfernt, auf die es abgesehen hat.
3. Informationen zum Löschen des VPC-Endpunkts, der diesem Security Agent zugeordnet ist, finden Sie unter. To delete a VPC endpoint

Bereinigen der Ressourcen des Security Agents

In diesem Abschnitt wird erklärt, wie Sie die mit dem Security Agent verknüpften AWS Ressourcen bereinigen können. Wie unter aufgeführtDeaktivierung, Deinstallation und Bereinigung der Ressourcen, GuardDuty werden nicht alle Security Agent-Ressourcen gelöscht oder entfernt. Der folgende Abschnitt enthält Anweisungen, wie Sie die Security Agent-Ressourcen löschen können.

So löschen Sie den Amazon VPC-Endpunkt

Wenn Sie den Security Agent manuell verwalten, haben Sie möglicherweise manuell einen Amazon VPC-Endpunkt erstellt. Nachdem Sie den Security Agent für alle überwachten Ressourcen in Ihrem Konto deinstalliert haben, können Sie diesen VPC-Endpunkt löschen.

Die folgende Liste enthält Szenarien für die Verwendung einer gemeinsam genutzten VPC im Vergleich zur Nichtverwendung einer gemeinsam genutzten VPC.

- Ohne eine gemeinsam genutzte VPC — Wenn Sie eine Ressource in einem Konto nicht mehr überwachen möchten, sollten Sie erwägen, den Amazon VPC-Endpunkt zu löschen.
- Mit einer gemeinsam genutzten VPC — Wenn ein gemeinsames VPC-Besitzerkonto die noch verwendete gemeinsame VPC-Ressource löscht, kann der Status der Runtime Monitoring-Abdeckung (und gegebenenfalls EKS Runtime Monitoring) für die Ressourcen in Ihrem gemeinsam genutzten VPC-Besitzerkonto und dem teilnehmenden Konto beeinträchtigt werden. Informationen zum Deckungsstatus finden Sie unter. Überprüfung der Statistiken zur Laufzeitabdeckung und Behebung von Problemen

Informationen zum Löschen des VPC-Endpunkts finden Sie im AWS PrivateLink Handbuch unter Löschen eines Schnittstellenendpunkts.

Um die Sicherheitsgruppe zu löschen

- Ohne eine gemeinsam genutzte VPC — Wenn Sie einen Ressourcentyp in einem Konto nicht mehr überwachen möchten, sollten Sie erwägen, die mit der Amazon VPC verknüpfte Sicherheitsgruppe zu löschen.
- Mit einer gemeinsam genutzten VPC — Wenn das gemeinsame VPC-Besitzerkonto die Sicherheitsgruppe löscht, kann es sein, dass alle Teilnehmerkonten, die derzeit die mit der gemeinsam genutzten VPC verknüpfte Sicherheitsgruppe verwenden, der Runtime Monitoring-Abdeckungsstatus für die Ressourcen in Ihrem gemeinsamen VPC-Besitzerkonto und dem teilnehmenden Konto fehlerhaft werden. Weitere Informationen finden Sie unter Überprüfung der Statistiken zur Laufzeitabdeckung und Behebung von Problemen.

Informationen zu den Schritten finden Sie unter Löschen einer Amazon EC2-Sicherheitsgruppe im Amazon EC2-Benutzerhandbuch.

Um den GuardDuty Security Agent aus einem EKS-Cluster zu entfernen

Informationen zum Entfernen des Security Agents aus Ihrem EKS-Cluster, den Sie nicht mehr überwachen möchten, finden Sie im Amazon EKS-Benutzerhandbuch unter Entfernen eines Amazon EKS-Add-ons aus einem Cluster.

Durch das Entfernen des EKS-Add-On-Agenten wird der `amazon-guardduty`-Namespace nicht aus dem EKS-Cluster entfernt. Um einen `amazon-guardduty`-Namespace zu löschen, sehen Sie Einen Namespace löschen.

Um den **`amazon-guardduty`** Namespace (EKS-Cluster) zu löschen

Durch das Deaktivieren der automatisierten Agentenkonfiguration wird der `amazon-guardduty` Namespace nicht automatisch aus Ihrem EKS-Cluster entfernt. Um einen `amazon-guardduty`-Namespace zu löschen, sehen Sie Einen Namespace löschen.

GuardDuty Malware-Schutz für EC2

Malware Protection for EC2 hilft Ihnen dabei, das potenzielle Vorhandensein von Malware zu erkennen, indem es die Amazon Elastic Block Store (Amazon EBS) -Volumes scannt, die an Amazon Elastic Compute Cloud (Amazon EC2) -Instances und Container-Workloads angehängt sind, die auf Amazon EC2 ausgeführt werden. Malware Protection for EC2 bietet Scanoptionen, mit denen Sie entscheiden können, ob Sie bestimmte Amazon EC2-Instances zum Zeitpunkt des Scannens ein- oder ausschließen möchten. Es bietet auch die Option, die Snapshots von Amazon EBS-Volumes, die an die Amazon EC2-Instances oder Container-Workloads angehängt sind, in Ihren Konten beizubehalten. GuardDuty Die Snapshots werden nur aufbewahrt, wenn Malware gefunden wird und die Ergebnisse von Malware Protection for EC2 generiert werden.

Malware Protection for EC2 wurde so konzipiert, dass die Leistung Ihrer Ressourcen nicht beeinträchtigt wird. Informationen zur Funktionsweise von Malware Protection for EC2 finden Sie unter GuardDuty. Wie werden EBS-Volumes zur Erkennung von Schadsoftware GuardDuty gescannt Informationen zur Verfügbarkeit von Malware Protection for EC2 in verschiedenen Versionen finden Sie AWS-Regionen unter. Regionen und Endpunkte

> **Hinweise**
>
> Malware Protection for EC2 unterstützt Malware-Scans auf verwalteten Instances für den Amazon EKS Auto Mode. Weitere Informationen finden Sie unter Unterstützung für verwaltete Instanzen in Guardduty.
> Malware Protection for EC2 unterstützt keine Malware-Scans für AWS Fargate Workloads, die entweder mit Amazon EKS oder Amazon ECS ausgeführt werden.
> Informationen zu diesen Amazon EKS-Funktionen finden Sie unter Was ist Amazon EKS? im Amazon EKS-Benutzerhandbuch .

Themen

- Vergleich von GuardDuty-initiated Malware-Scan und On-demand Malware-Scan
- Wie werden EBS-Volumes zur Erkennung von Schadsoftware GuardDuty gescannt
- Unterstützte Amazon EBS-Volumes für den Malware-Scan
- Richten Sie die Snapshot-Aufbewahrung und die EC2-Scanabdeckung ein
- GuardDuty-initiated Malware-Scan
- On-demand Malware-Scan in GuardDuty

- Überwachung des Scanstatus und der Ergebnisse in Malware Protection for EC2
- GuardDuty Dienstkonten von AWS-Region
- Kontingente im Malware-Schutz für EC2

Vergleich von GuardDuty-initiated Malware-Scan und On-demand Malware-Scan

Malware Protection for EC2 bietet zwei Arten von Scans zur Erkennung potenziell bösartiger Aktivitäten in Ihren Amazon EC2-Instances und Container-Workloads: GuardDuty-initiated Malware-Scan und On-demand Malware-Scan. Die folgende Tabelle zeigt den Vergleich zwischen den beiden Scan-Typen.

Faktor	GuardDuty-initiated Malware-Scan	On-demand Malware-Scan
Wie der Scan aufgerufen wird	Nachdem Sie den GuardDuty-initiated Malware-Scan aktiviert haben, GuardDuty initiiert jedes Mal, wenn ein Befund generiert wird, der auf das potenzielle Vorhandensein von Malware in einer Amazon EC2-Instance oder einem Container-Workload hinweist, GuardDuty automatisch einen agentenlosen Malware-Scan auf den Amazon EBS-Volumes, die an Ihre potenziell betroffene Ressource angeschlossen sind. Weitere Informationen finden Sie unter GuardDuty-initiated Malware-Scan.	Sie können einen On-demand Malware-Scan initiieren, indem Sie den Amazon-Ressourcennamen (ARN) Ihrer Amazon EC2-Instance angeben. Sie können einen On-demand Malware-Scan auch dann einleiten, wenn für Ihre Ressource kein GuardDuty Ergebnis generiert wurde. Weitere Informationen finden Sie unter On-demand Malware-Scan in GuardDuty.
Konfiguration erforderlich	Um den GuardDuty-initiated Malware-Scan verwenden zu	Ihr Konto muss GuardDuty aktiviert sein. Um den On-

Faktor	GuardDuty-initiated Malware-Scan	On-demand Malware-Scan
	können, müssen Sie ihn für Ihr Konto aktivieren. Informationen zur Verwaltung mehrerer Konten mithilfe einer AWS Organizations einladungsbasierten Methode finden Sie unter Aktivierung des GuardDuty-initiated Malware-Scans in Umgebungen mit mehreren Konten. Informationen zur Aktivierung des GuardDuty-initiated Malware-Scans in Ihrem eigenen Konto finden Sie unter Aktivierung des GuardDuty-initiated Malware-Scans für ein eigenständiges Konto.	demand Malware-Scan zu verwenden, ist auf Funktionsebene keine Konfiguration erforderlich.
Wartezeit zum Initiieren eines neuen Scanvorgangs	Immer wenn ein Malware-Scan GuardDuty generiert wird Ergebnisse, die den GuardDuty-initiated Malware-Scan auslösen, wird ein Malware-Scan automatisch nur einmal alle 24 Stunden gestartet.	Sie können jederzeit einen On-demand Malware-Scan auf derselben Ressource starten, nachdem der vorherige Scan eine Stunde später gestartet wurde.

Faktor	GuardDuty-initiated Malware-Scan	On-demand Malware-Scan
Verfügbarkeit der kostenlosen 30-tägigen Testphase [1]	Wenn Sie den GuardDuty-initiated Malware-Scan zum ersten Mal in Ihrem Konto aktivieren, können Sie eine 30-tägige kostenlose Testphase nutzen. Weitere Informationen finden Sie unter Kostenlose 30-Tage-Testversion im GuardDuty-initiated Malware-Scan.	Es gibt keinen kostenlosen Testzeitraum für den On-demand Malware-Scan für neue oder bestehende GuardDuty Konten.
Optionen zum Scannen [2]	Nachdem Sie den GuardDuty-initiated Malware-Scan konfiguriert haben, bietet Malware Protection for EC2 die Möglichkeit, bestimmte Amazon EC2-Ressourcen mithilfe von Tags zu scannen oder zu überspringen. Malware Protection for EC2 initiiert keinen automatischen Scan der Ressourcen, die Sie vom Scannen ausschließen möchten. Weitere Informationen finden Sie unter Scan-Optionen mit benutzerdefinierten Tags.	Da Sie den Ressourcen-ARN angeben, um einen On-Demand-Malware-Scan manuell zu starten, Scan-Optionen mit benutzerdefinierten Tags ist die Verwendung nicht möglich.

[1] Für die Erstellung und Aufbewahrung von EBS-Volume-Snapshots fallen Nutzungskosten an. Weitere Informationen zur Konfiguration Ihres Kontos für die Aufbewahrung von Snapshots finden Sie unter. Snapshot-Beibehaltung

[2] Sowohl der GuardDuty-initiated Malware-Scan als auch der On-demand Malware-Scan unterstützen die Verwendung eines globalen Tags, um Amazon EC2-Ressourcen von Malware-Scans auszuschließen. Weitere Informationen finden Sie unter Globales `GuardDutyExcluded`-Tag.

Wie werden EBS-Volumes zur Erkennung von Schadsoftware GuardDuty gescannt

In diesem Abschnitt wird erklärt, wie Malware Protection for EC2, einschließlich GuardDuty-initiated Malware-Scan und On-demand Malware-Scan, die Amazon EBS-Volumes scannt, die Ihren Amazon EC2-Instances und Container-Workloads zugeordnet sind. Berücksichtigen Sie die folgenden Anpassungen, bevor Sie fortfahren:

- Scanoptionen — Malware Protection for EC2 bietet die Möglichkeit, Tags anzugeben, um Amazon EC2-Instances und Amazon EBS-Volumes entweder in den Scanvorgang einzubeziehen oder auszuschließen. Nur der GuardDuty-initiated Malware-Scan unterstützt Scanoptionen mit benutzerdefinierten Tags. Sowohl der GuardDuty-initiated Malware-Scan als auch der On-demand Malware-Scan unterstützen das globale `GuardDutyExcluded` Tag. Weitere Informationen finden Sie unter Scan-Optionen mit benutzerdefinierten Tags.
- Aufbewahrung von Snapshots — Malware Protection for EC2 bietet die Option, die Snapshots Ihrer Amazon EBS-Volumes in Ihrem Konto aufzubewahren. AWS Diese Einstellung ist standardmäßig deaktiviert. Sie können die Aufbewahrung von Snapshots sowohl für GuardDuty initiierte als auch für On-Demand-Malware-Scans aktivieren. Weitere Informationen finden Sie unter Snapshot-Beibehaltung.

Wenn ein oder mehrere GuardDuty generiert werdenErgebnisse, die den GuardDuty-initiated Malware-Scan auslösen, ist diese Aktivität ein Grund GuardDuty , einen Malware-Scan einzuleiten. Wenn Ihre Scanoptionen diese Instanz nicht ausschließen, GuardDuty wird der Scan gestartet.

Um einen On-demand Malware-Scan auf den Amazon EBS-Volumes zu starten, die einer Amazon EC2-Instance zugeordnet sind, geben Sie den Amazon-Ressourcennamen (ARN) der Amazon EC2-Instance an.

Als Reaktion auf den Start eines On-Demand-Malware-Scans oder eines automatischen GuardDuty-initiated Malware-Scans werden Snapshots der relevanten EBS-Volumes GuardDuty erstellt, die an die potenziell betroffene Ressource angehängt sind, und gibt sie an die weiter. GuardDuty Dienstkonto Wenn GuardDuty ein Snapshot Ihrer EBS-Volumes erstellt wird, wird ein Standard-Tag mit dem Namen hinzugefügt. `GuardDutyScanId` Dieses Tag hilft beim GuardDuty Zugriff auf den

Snapshot. Stellen Sie sicher, dass Sie dieses Tag nicht entfernen. GuardDuty Erstellt aus diesen Snapshots ein verschlüsseltes Replikat-EBS-Volume im Dienstkonto.

GuardDuty Löscht nach Abschluss des Scans die verschlüsselten Replikat-EBS-Volumes und die Snapshots Ihrer EBS-Volumes. Die Einstellung zur Aufbewahrung von Snapshots ist standardmäßig deaktiviert. Snapshots werden jedoch unabhängig von den Scanergebnissen und Einstellungen aufbewahrt, wenn die Amazon EBS-Snapshot-Sperre für sie aktiviert ist. GuardDuty kann die Amazon EBS-Snapshot-Sperreinstellungen nicht ändern.

In der folgenden Liste wird das Aufbewahrungsverhalten von Snapshots beschrieben, unabhängig vom Sperren von EBS-Snapshots:

Die Aufbewahrung von Snapshots ist aktiviert:

- Wenn Malware gefunden wird, werden die GuardDuty Snapshots in Ihrem gespeichert. AWS-Konto
- Wenn keine Malware gefunden wird, GuardDuty werden die Snapshots nur gespeichert, wenn sie gesperrt sind.

Die Aufbewahrung von Snapshots ist deaktiviert (Standardeinstellung):

- Unabhängig davon, ob Malware gefunden wird oder nicht, werden die Snapshots nicht aufbewahrt.
- GuardDuty gesperrte Amazon EBS-Snapshots können nicht gelöscht werden.

GuardDuty speichert jedes Replikat-EBS-Volume bis zu 55 Stunden lang im Servicekonto. Bei einem Serviceausfall oder einem Ausfall eines Replikat-EBS-Volumes und des zugehörigen Malware-Scans GuardDuty wird ein solches EBS-Volume nicht länger als sieben Tage aufbewahrt. Die verlängerte Speicherfrist dient dazu, den Ausfall oder Ausfall zu analysieren und zu beheben. GuardDuty Malware Protection for EC2 löscht die replizierten EBS-Volumes aus dem Dienstkonto, nachdem der Ausfall oder Ausfall behoben wurde oder die erweiterte Aufbewahrungsfrist abgelaufen ist.

Informationen zur GuardDuty Malware-Erkennungsmethode und zu den verwendeten Scan-Engines finden Sie unter. GuardDuty Scan-Engine zur Malware-Erkennung

Unterstützte Amazon EBS-Volumes für den Malware-Scan

In allen Bereichen, in AWS-Regionen denen die Funktion Malware Protection for EC2 GuardDuty unterstützt wird, können Sie die Amazon EBS-Volumes scannen, die unverschlüsselt oder

verschlüsselt sind. Sie können Amazon EBS-Volumes verwenden, die entweder mit einem Von AWS verwalteter Schlüssel oder einem vom Kunden verwalteten Schlüssel verschlüsselt sind. Derzeit unterstützen einige Regionen, in denen Malware Protection for EC2 verfügbar ist, möglicherweise beide Arten der Verschlüsselung Ihrer Amazon EBS-Volumes, während andere nur vom Kunden verwaltete Schlüssel unterstützen. Informationen zu den unterstützten Regionen finden Sie unter und. GuardDuty Dienstkonten von AWS-Region Informationen zu Regionen, in denen GuardDuty zwar verfügbar, aber Malware Protection for EC2 nicht verfügbar ist, finden Sie unterRegion-specific Verfügbarkeit von Funktionen.

In der folgenden Liste wird der Schlüssel beschrieben, der GuardDuty verwendet, unabhängig davon, ob Ihre Amazon EBS-Volumes verschlüsselt sind oder nicht:

- Amazon EBS-Volumes, die entweder unverschlüsselt oder mit Von AWS verwalteter Schlüssel — verschlüsselt sind, GuardDuty verwendet ihren eigenen Schlüssel, um die Replikat-Amazon EBS-Volumes zu verschlüsseln.

  Wenn Ihre Region das Scannen von Amazon EBS-Volumes, die standardmäßig mit Amazon EBS-Verschlüsselung verschlüsselt sind, nicht unterstützt, müssen Sie den Standardschlüssel so ändern, dass er ein vom Kunden verwalteter Schlüssel ist. Dies hilft beim GuardDuty Zugriff auf diese EBS-Volumes. Durch die Änderung des Schlüssels werden sogar zukünftige EBS-Volumes mit dem aktualisierten Schlüssel erstellt, sodass Malware-Scans unterstützt werden GuardDuty können. Schritte zum Ändern des Standardschlüssels finden Sie Standard ändern AWS KMS Schlüssel-ID eines Amazon EBS-Volumes im nächsten Abschnitt.
- Amazon EBS-Volumes, die mit einem vom Kunden verwalteten Schlüssel verschlüsselt sind — GuardDuty verwendet denselben Schlüssel, um das Replikat-EBS-Volume zu verschlüsseln. Informationen darüber, welche AWS KMS Verschlüsselungsrichtlinien unterstützt werden, finden Sie unter. Service-linked Rollenberechtigungen für Malware Protection for EC2

Standard ändern AWS KMS Schlüssel-ID eines Amazon EBS-Volumes

Wenn Sie mithilfe der Amazon EBS-Verschlüsselung ein Amazon EBS-Volume erstellen verwenden und keine AWS KMS Schlüssel-ID angeben, wird Ihr Amazon EBS-Volume mit einem Standardschlüssel für die Verschlüsselung verschlüsselt. Wenn Sie die Verschlüsselung standardmäßig aktivieren, verschlüsselt Amazon EBS automatisch neue Volumes und Snapshots mithilfe Ihres Standard-KMS-Schlüssels für die Amazon EBS-Verschlüsselung.

Sie können den Standardverschlüsselungsschlüssel ändern und einen vom Kunden verwalteten Schlüssel für die Amazon EBS-Verschlüsselung verwenden. Dies hilft beim GuardDuty Zugriff auf

diese Amazon EBS-Volumes. Um die EBS-Standardschlüssel-ID zu ändern, fügen Sie Ihrer IAM-Richtlinie die folgende erforderliche Berechtigung hinzu: `ec2:modifyEbsDefaultKmsKeyId`. Jedes neu erstellte Amazon EBS-Volume, das Sie für die Verschlüsselung auswählen, aber keine zugehörige KMS-Schlüssel-ID angeben, verwendet die Standard-Schlüssel-ID. Verwenden Sie eine der folgenden Methoden, um die EBS-Standardschlüssel-ID zu aktualisieren:

So ändern Sie die standardmäßige KMS-Schlüssel-ID eines Amazon-EBS-Volumes

Führen Sie eine der folgenden Aktionen aus:

- Verwendung einer API — Sie können die ModifyEbsDefaultKmsKeyId API verwenden. Informationen darüber, wie Sie den Verschlüsselungsstatus Ihres Volumes einsehen können, finden Sie unter Amazon EBS-Volume https://docs.aws.amazon.com/ erstellen.
- AWS CLI Befehl verwenden — Im folgenden Beispiel wird die standardmäßige KMS-Schlüssel-ID geändert, mit der Amazon EBS-Volumes verschlüsselt werden, wenn Sie keine KMS-Schlüssel-ID angeben. Stellen Sie sicher, dass Sie die Region durch die Ihrer AWS-Region KM-Schlüssel-ID ersetzen.

  ```
  aws ec2 modify-ebs-default-kms-key-id --region us-west-2 --kms-key-
  id AKIAIOSFODNN7EXAMPLE
  ```

  Der obige Befehl wird eine Ausgabe erzeugen, die folgendermaßen aussieht:

  ```
  {
    "KmsKeyId": "arn:aws:kms:us-west-2:444455556666:key/AKIAIOSFODNN7EXAMPLE"
  }
  ```

  Weitere Informationen finden Sie unter modify-ebs-default-kms-key-id.

Richten Sie die Snapshot-Aufbewahrung und die EC2-Scanabdeckung ein

In diesem Abschnitt wird erklärt, wie Sie die Malware-Scanoptionen für Ihre Amazon EC2-Instances anpassen. Diese Anpassungen gelten sowohl für On-demand Malware-Scans als auch für solche, die von initiiert wurden. GuardDuty Sie haben die folgenden Möglichkeiten:

- Snapshot-Aufbewahrung aktivieren — Wenn diese Option vor einem Scan aktiviert ist, GuardDuty wird der Amazon EBS-Snapshot beibehalten, der als bösartig GuardDuty erkannt wurde.

- Wählen Sie aus, welche Amazon EC2-Instances gescannt werden sollen — Verwenden Sie Tags, um bestimmte Amazon EC2-Instances in Malware-Scans ein- oder auszuschließen.

Snapshot-Beibehaltung

GuardDuty bietet Ihnen die Möglichkeit, die Snapshots Ihrer EBS-Volumes in Ihrem Konto zu speichern. AWS Standardmäßig ist die Aufbewahrungseinstellung für Snapshots deaktiviert. Die Snapshots werden nur beibehalten, wenn Sie diese Einstellung aktiviert haben, bevor der Scan gestartet wird.

GuardDuty Generiert zu Beginn des Scans die Replikat-EBS-Volumes auf der Grundlage der Snapshots Ihrer EBS-Volumes. Nachdem der Scan abgeschlossen ist und die Einstellung zur Aufbewahrung von Snapshots in Ihrem Konto bereits aktiviert wurde, werden die Snapshots Ihrer EBS-Volumes nur beibehalten, wenn Malware gefunden und Malware-Schutz für EC2-Suchtypen generiert wird. Wenn keine Malware gefunden wird, werden unabhängig von Ihren Snapshot-Einstellungen GuardDuty automatisch die Snapshots Ihrer EBS-Volumes gelöscht, es sei denn, die Amazon EBS-Snapshot-Sperre wurde für die erstellten Snapshots aktiviert.

Nutzungskosten für Snapshots

Während des Malware-Scannens, bei dem die Snapshots Ihrer Amazon EBS-Volumes GuardDuty erstellt werden, fallen mit diesem Schritt Nutzungskosten an. Wenn Sie die Einstellung zur Aufbewahrung von Snapshots für Ihr Konto aktivieren, fallen für Sie Nutzungskosten an, wenn Malware gefunden wird und die Snapshots beibehalten werden. Informationen zu den Kosten von Snapshots und deren Aufbewahrung finden Sie unter Amazon EBS-Preise.

Als delegiertes GuardDuty Administratorkonto können nur Sie diese Aktualisierung im Namen der Mitgliedskonten der Organisation vornehmen. Wenn ein Mitgliedskonto jedoch nach der Einladungsmethode verwaltet wird, kann das Mitglied diese Änderung selbst vornehmen. Weitere Informationen finden Sie unter Beziehungen zwischen Administratorkonto und Mitgliedskonto.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um die Aufbewahrungseinstellung für Snapshots zu aktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich unter Schutzpläne die Option Malware Protection for EC2 aus.

3. Wählen Sie im unteren Bereich der Konsole Allgemeine Einstellungen. Um die Snapshots beizubehalten, aktivieren Sie die Option Beibehaltung von Snapshots.

API/CLI

Führen Sie UpdateMalwareScanSettings diese Option aus, um die aktuelle Konfiguration für die Einstellung zur Aufbewahrung von Snapshots zu aktualisieren.

Alternativ können Sie den folgenden AWS CLI Befehl ausführen, um Snapshots automatisch aufzubewahren, wenn GuardDuty Malware Protection for EC2 Ergebnisse generiert.

Stellen Sie sicher, dass Sie das durch Ihr *detector-id* eigenes gültiges ersetzen. `detectorId`

Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625554d637e0e4bb3b2 --ebs-snapshot-preservation
 "RETENTION_WITH_FINDING"
```

Wenn Sie die Beibehaltung von Snapshots deaktivieren möchten, ersetzen Sie sie `RETENTION_WITH_FINDING` durch `NO_RETENTION`.

Scan-Optionen mit benutzerdefinierten Tags

Mithilfe des GuardDuty-initiated Malware-Scans können Sie auch Tags angeben, um Amazon EC2-Instances und Amazon EBS-Volumes in den Scan- und Bedrohungserkennungsprozess einzubeziehen oder auszuschließen. Sie können jeden GuardDuty-initiated Malware-Scan individuell anpassen, indem Sie die Tags entweder in der Liste der Einschluss- oder Ausschluss-Tags bearbeiten. Jede Liste kann bis zu 50 Tags enthalten.

Wenn Ihren EC2-Ressourcen noch keine benutzerdefinierten Tags zugeordnet sind, finden Sie weitere Informationen unter Markieren Ihrer Amazon EC2-Ressourcen im Amazon EC2-Benutzerhandbuch.

> **Note**
>
> On-demand Der Malware-Scan unterstützt keine Scanoptionen mit benutzerdefinierten Tags. Er unterstützt Globales `GuardDutyExcluded`-Tag.

So schließen Sie EC2-Instances vom Malware-Scan aus

Wenn Sie eine Amazon EC2-Instance oder ein Amazon EBS-Volume während des Scanvorgangs ausschließen möchten, können Sie das `GuardDutyExcluded` Tag `true` für jede Amazon EC2-Instance oder jedes Amazon EBS-Volume auf setzen und GuardDuty es wird nicht gescannt. Weitere Informationen über das `GuardDutyExcluded`-Tag finden Sie unter Service-linked Rollenberechtigungen für Malware Protection for EC2. Sie können auch ein Amazon-EC2-Instance-Tag zu einer Ausschlussliste hinzufügen. Wenn Sie der Liste der Ausschluss-Tags mehrere Tags hinzufügen, wird jede Amazon-EC2-Instance, die mindestens eines dieser Tags enthält, vom Malware-Scanvorgang ausgeschlossen.

Als delegiertes GuardDuty Administratorkonto können nur Sie diese Aktualisierung im Namen der Mitgliedskonten der Organisation vornehmen. Wenn ein Mitgliedskonto jedoch nach der Einladungsmethode verwaltet wird, kann das Mitglied diese Änderung selbst vornehmen. Weitere Informationen finden Sie unter Beziehungen zwischen Administratorkonto und Mitgliedskonto.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um ein mit einer Amazon-EC2-Instance verknüpftes Tag zu einer Ausschlussliste hinzuzufügen.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich unter Schutzpläne die Option Malware Protection for EC2 aus.
3. Erweitern Sie den Abschnitt mit den Inclusion/Exclusion Stichwörtern. Wählen Sie Tags hinzufügen aus.
4. Wählen Sie Ausschluss-Tags und anschließend Bestätigen.
5. Geben Sie das **`Key`**- und **`Value`**-Paar des Tags an, das Sie ausschließen möchten. Die Angabe von **`Value`** ist optional. Nachdem Sie alle Tags hinzugefügt haben, wählen Sie Speichern.

> **Important**
>
> Bei Tag-Schlüsseln und -Werten wird zwischen Groß- und Kleinschreibung unterschieden. Weitere Informationen finden Sie unter Tag-Einschränkungen im Amazon EC2-Benutzerhandbuch.

Wenn kein Wert für einen Schlüssel angegeben wird und die EC2-Instance mit dem angegebenen Schlüssel gekennzeichnet ist, wird diese EC2-Instance unabhängig vom GuardDuty-initiated zugewiesenen Wert des Tags vom Malware-Scanvorgang ausgeschlossen.

API/CLI

Wird ausgeführt, UpdateMalwareScanSettings indem eine EC2-Instance oder ein Container-Workload vom Scanvorgang ausgeschlossen wird.

Mit dem folgenden AWS CLI Beispielbefehl wird der Liste der Ausnahmetags ein neues Tag hinzugefügt. Ersetzen Sie das Beispiel *detector-id* durch Ihre eigene gültige `detectorId`.

`MapEquals` ist eine Liste von `Key`/`Value`-Paaren.

Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625 54d637e0e4bb3b2 --scan-resource-criteria '{"Exclude":
 {"EC2_INSTANCE_TAG" : {"MapEquals": [{ "Key": "TestKeyWithValue", "Value":
 "TestValue" }, {"Key":"TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation
 "RETENTION_WITH_FINDING"
```

> **Important**
>
> Bei Tag-Schlüsseln und -Werten wird zwischen Groß- und Kleinschreibung unterschieden. Weitere Informationen finden Sie unter Tag-Einschränkungen im Amazon EC2-Benutzerhandbuch.

So schließen Sie EC2-Instances in den Malware-Scan ein

Wenn Sie eine EC2-Instance scannen möchten, fügen Sie ihr Tag zur Einschluss-Liste hinzu. Wenn Sie ein Tag zu einer Liste mit Einschluss-Tags hinzufügen, wird eine EC2-Instance, die keines der hinzugefügten Tags enthält, aus dem Malware-Scan übersprungen. Wenn Sie der Liste der Einschluss-Tags mehrere Tags hinzufügen, wird eine EC2-Instance, die mindestens eines dieser Tags enthält, in den Malware-Scan aufgenommen. Manchmal kann eine EC2-Instance aus anderen Gründen während des Scanvorgangs übersprungen werden. Weitere Informationen finden Sie unter Gründe für das Überspringen von Ressourcen beim Malware-Scan.

Als delegiertes GuardDuty Administratorkonto können nur Sie diese Aktualisierung im Namen der Mitgliedskonten der Organisation vornehmen. Wenn ein Mitgliedskonto jedoch nach der Einladungsmethode verwaltet wird, kann das Mitglied diese Änderung selbst vornehmen. Weitere Informationen finden Sie unter Beziehungen zwischen Administratorkonto und Mitgliedskonto.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um ein mit einer Amazon-EC2-Instance verknüpftes Tag zu einer Einschlussliste hinzuzufügen.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich unter Schutzpläne die Option Malware Protection for EC2 aus.
3. Erweitern Sie den Abschnitt mit den Inclusion/Exclusion Stichwörtern. Wählen Sie Tags hinzufügen aus.
4. Wählen Sie Einschluss-Tags und dann Bestätigen.
5. Wählen Sie Neues Einschluss-Tag hinzufügen und geben Sie das **`Key`**- und **`Value`**-Paar des Tags an, das Sie einbeziehen möchten. Die Angabe von **`Value`** ist optional.

   Nachdem Sie alle Einschluss-Tags hinzugefügt haben, wählen Sie Speichern.

   Wenn kein Wert für einen Schlüssel angegeben wird, wird eine EC2-Instance mit dem angegebenen Schlüssel markiert, wird die EC2-Instance unabhängig vom zugewiesenen Wert des Tags in den Malware-Schutz für EC2-Scanvorgang einbezogen.

API/CLI

- Führen Sie diesen UpdateMalwareScanSettings Befehl aus, um eine EC2-Instance oder einen Container-Workload in den Scanvorgang einzubeziehen.

  Mit dem folgenden AWS CLI Beispielbefehl wird der Liste der Inklusionstags ein neues Tag hinzugefügt. Stellen Sie sicher, dass Sie das Beispiel durch Ihr *detector-id* eigenes gültiges Beispiel ersetzen`detectorId`. Ersetzen Sie das Beispiel *TestKey* und *TestValue* durch das `Value` Paar `Key` und des Tags, das Ihrer EC2-Ressource zugeordnet ist.

  `MapEquals` ist eine Liste von `Key`/`Value`-Paaren.

  Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

  ```
  aws guardduty update-malware-scan-settings --detector-
  id 60b87779336485625 54d637e0e4bb3b2 --scan-resource-criteria '{"Include":
   {"EC2_INSTANCE_TAG" : {"MapEquals": [{ "Key": "TestKeyWithValue", "Value":
   "TestValue" }, {"Key":"TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation
   "RETENTION_WITH_FINDING"
  ```

  Important

  Bei Tag-Schlüsseln und -Werten wird zwischen Groß- und Kleinschreibung unterschieden. Weitere Informationen finden Sie unter Tag-Einschränkungen im Amazon EC2-Benutzerhandbuch.

Note

Es kann bis zu 5 Minuten dauern, GuardDuty bis ein neues Tag erkannt wird.

Sie können jederzeit entweder Einschluss-Tags oder Ausschluss-Tags wählen, aber nicht beides. Wenn Sie zwischen den Tags wechseln möchten, wählen Sie dieses Tag aus dem Drop-down-Menü aus, wenn Sie neue Tags hinzufügen, und Bestätigen Sie Ihre Auswahl. Diese Aktion löscht alle Ihre aktuellen Tags.

Globales **GuardDutyExcluded**-Tag

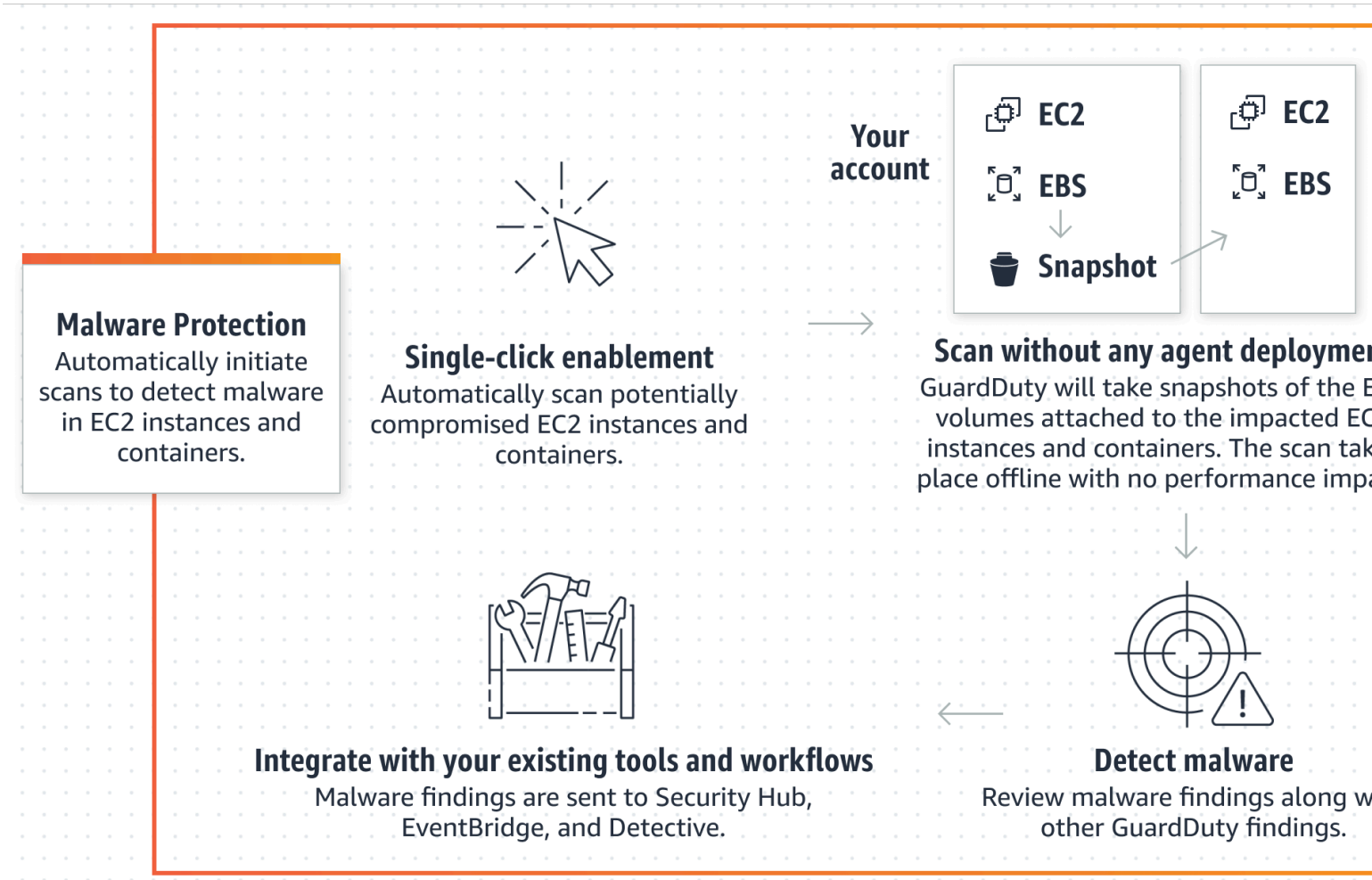
GuardDuty verwendet einen globalen Tag-Schlüssel`GuardDutyExcluded`, den Sie zu Ihren Amazon EC2-Ressourcen hinzufügen und den Tag-Wert auf `true` setzen können. Diese Amazon EC2-Ressource, die über dieses Tag-Schlüssel-Wert-Paar verfügt, wird vom Malware-Scan ausgeschlossen. Beide Scantypen (GuardDuty-initiated Malware-Scan und On-demand Malware-Scan) unterstützen das globale Tag. Wenn Sie einen On-Demand-Malware-Scan auf einem Amazon EC2 starten, wird eine Scan-ID generiert. Der Scan wird jedoch mit einem `EXCLUDED_BY_SCAN_SETTINGS` Grund übersprungen. Weitere Informationen finden Sie unter Gründe für das Überspringen von Ressourcen beim Malware-Scan.

GuardDuty-initiated Malware-Scan

Wenn der GuardDuty-initiated Malware-Scan aktiviert ist, wird bei jedem GuardDuty Ergebnisse, die den GuardDuty-initiated Malware-Scan auslösen Generierungsvorgang ein agentenloser Malware-Scan auf den Amazon Elastic Block Store (Amazon EBS) -Volumes eingeleitet, die an die potenziell betroffene Amazon EC2-Ressource angeschlossen sind. Bevor ein Scan gestartet wird, müssen Sie Ihr Konto für alle Anpassungen vorbereiten. Mit den Scanoptionen können Sie Einschluss-Tags hinzufügen, die den Ressourcen zugeordnet sind, die Sie scannen möchten, oder Ausschluss-Tags hinzufügen, die den Ressourcen zugeordnet sind, die Sie beim Scanvorgang überspringen möchten. Bei der automatischen Initiierung eines Scans werden immer Ihre Scanoptionen berücksichtigt. GuardDuty unterstützt auch ein globales`GuardDutyExcluded`: `true` -Tag-Schlüssel:Wert-Paar. Wenn Sie dieses globale Tag zu einer Amazon EC2-Ressource hinzufügen, GuardDuty wird der Scan gestartet und dann übersprungen. Sie können auch die Einstellung zur Aufbewahrung von Snapshots aktivieren, um die Snapshots Ihrer EBS-Volumes beizubehalten, auf denen potenziell Malware entdeckt wurde. Weitere Informationen zu den Scanoptionen, dem globalen Ausschluss-Tag und den Snapshot-Einstellungen finden Sie unter. Richten Sie die Snapshot-Aufbewahrung und die EC2-Scanabdeckung ein

Wenn mehrere Ergebnisse für dieselbe Amazon EC2-Ressource GuardDuty generiert GuardDuty werden, kann ein Scan erst gestartet werden, nachdem 24 Stunden seit dem letzten GuardDuty-initiated Malware-Scan vergangen sind. Informationen darüber, wie die Amazon-EBS-Volumes gescannt werden, die Ihrer Amazon-EC2-Instance oder Ihrem Container-Workload zugeordnet sind, finden Sie unter Wie werden EBS-Volumes zur Erkennung von Schadsoftware GuardDuty gescannt.

Die folgende Abbildung beschreibt, wie der GuardDuty-initiated Malware-Scan funktioniert.



Informationen zur GuardDuty Malware-Erkennungsmethode und zu den dabei verwendeten Scan-Engines finden Sie unter. GuardDuty Scan-Engine zur Malware-Erkennung

Wenn Schadsoftware gefunden wird, wird GuardDuty generiertMalware-Schutz für EC2-Suchtypen. Wenn GuardDuty kein Ergebnis generiert wird, das auf Malware auf derselben Ressource hinweist, wird kein GuardDuty-initiated Malware-Scan ausgeführt. Sie können auch einen On-demand Malware-Scan für dieselbe Ressource starten. Weitere Informationen finden Sie unter On-demand Malware-Scan in GuardDuty.

Kostenlose 30-Tage-Testversion im GuardDuty-initiated Malware-Scan

Sie können jederzeit wählen, ob Sie den GuardDuty-initiated Malware-Scan für ein AWS-Konto unterstütztes AWS-Region Gerät aktivieren oder deaktivieren möchten. Wenn Sie eine Organisation haben, hat jedes Mitgliedskonto eine eigene kostenlose 30-Tage-Testversion.

Um zu verstehen, wie die kostenlose 30-Tage-Testversion funktioniert, sollten Sie die folgenden Szenarien in Betracht ziehen:

- GuardDuty Bei der ersten Aktivierung (neues GuardDuty Konto) wird auch der GuardDuty-initiated Malware-Scan aktiviert und ist in der 30-Tage-Testversion des GuardDuty Dienstes enthalten.
- Ein vorhandenes GuardDuty Konto kann den GuardDuty-initiated Malware-Scan im Rahmen einer kostenlosen 30-Tage-Testversion zum ersten Mal aktivieren. Wenn Sie diese Funktion zum ersten Mal in einer anderen Region aktivieren, erhalten Sie in dieser Region eine kostenlose 30-Tage-Testversion.
- Wenn Sie Malware Protection for EC2 in einer Zeit verwendet haben, in AWS-Region der dieser Schutzplan in zwei Scantypen aufgeteilt wurde — GuardDuty-initiated Malware-Scan und On-demand Malware-Scan —, können Sie den GuardDuty-initiated Malware-Scan weiterhin mit demselben Preismodell und demselben Preismodell verwenden. AWS-Region Wenn Sie den GuardDuty-initiated Malware-Scan zum ersten Mal in einer neuen Region aktivieren, erhalten Sie für Ihr Konto eine kostenlose 30-Tage-Testversion.

> **Note**
>
> Selbst wenn Sie eine 30-tägige kostenlose Testphase haben, fallen die Standardnutzungskosten für die Erstellung der Amazon EBS-Volume-Snapshots und deren Aufbewahrung an. Weitere Informationen finden Sie unter Amazon EBS – Preise.

Aktivierung des GuardDuty-initiated Malware-Scans in Umgebungen mit mehreren Konten

In einer Umgebung mit mehreren Konten kann nur ein GuardDuty Administratorkonto den GuardDuty-initiated Malware-Scan im Namen seiner Mitgliedskonten aktivieren. Darüber hinaus kann ein Administratorkonto, das die Mitgliedskonten beim AWS Organizations Support verwaltet, festlegen, dass der GuardDuty-initiated Malware-Scan für alle vorhandenen und neuen Konten in der Organisation automatisch aktiviert wird. Weitere Informationen finden Sie unter GuardDuty Konten verwalten mit AWS Organizations.

Einrichtung eines vertrauenswürdigen Zugriffs zur Aktivierung des GuardDuty-initiated Malware-Scans

Wenn das Konto des GuardDuty delegierten Administrators nicht mit dem Verwaltungskonto in Ihrer Organisation identisch ist, muss das Verwaltungskonto die GuardDuty-initiated Malware-Suche für die Organisation aktivieren. Auf diese Weise kann das delegierte Administratorkonto die Service-linked Rollenberechtigungen für Malware Protection for EC2 Mitgliedskonten erstellen, über die verwaltet werden. AWS Organizations

> **Note**
>
> Bevor Sie ein delegiertes GuardDuty Administratorkonto einrichten, finden Sie weitere Informationen unter. Überlegungen und Empfehlungen

Wählen Sie Ihre bevorzugte Zugriffsmethode, damit das Konto des delegierten GuardDuty Administrators die GuardDuty-initiated Malware-Suche für Mitgliedskonten in der Organisation aktivieren kann.

Console

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

   Um sich anzumelden, verwenden Sie das Verwaltungskonto für Ihre AWS Organizations Organisation.

2. a. Wenn Sie kein delegiertes GuardDuty Administratorkonto eingerichtet haben, gehen Sie wie folgt vor:

      Geben Sie auf der Seite Einstellungen unter Konto für delegierte GuardDuty Administratoren die 12-stellige Zahl ein, **`account ID`** die Sie für die Verwaltung der GuardDuty Richtlinie in Ihrer Organisation festlegen möchten. Wählen Sie Delegieren.

   b. i. Wenn Sie bereits ein delegiertes GuardDuty Administratorkonto festgelegt haben, das sich vom Verwaltungskonto unterscheidet, gehen Sie wie folgt vor:

      Aktivieren Sie auf der Seite Einstellungen unter Delegierter Administrator die Einstellung Berechtigungen. Diese Aktion ermöglicht es dem delegierten GuardDuty Administratorkonto, den Mitgliedskonten entsprechende Berechtigungen zuzuweisen und den GuardDuty-initiated Malware-Scan in diesen Mitgliedskonten zu aktivieren.

ii. Wenn Sie bereits ein delegiertes GuardDuty Administratorkonto festgelegt haben, das mit dem Verwaltungskonto identisch ist, können Sie den GuardDuty-initiated Malware-Scan direkt für die Mitgliedskonten aktivieren. Weitere Informationen finden Sie unter Auto-enable GuardDuty-initiated Malware-Scan für alle Mitgliedskonten.

> **Tip**
>
> Wenn sich das delegierte GuardDuty Administratorkonto von Ihrem Verwaltungskonto unterscheidet, müssen Sie dem delegierten GuardDuty Administratorkonto Berechtigungen gewähren, damit die GuardDuty-initiated Malware-Suche für Mitgliedskonten aktiviert werden kann.

3. Wenn Sie zulassen möchten, dass das Konto des delegierten GuardDuty Administrators die GuardDuty-initiated Malware-Suche für Mitgliedskonten in anderen Regionen aktiviert, ändern Sie Ihre AWS-Region und wiederholen Sie die obigen Schritte.

API/CLI

1. Mit den Anmeldeinformationen für Ihr Verwaltungskonto führen Sie den folgenden Befehl aus:

```
aws organizations enable-aws-service-access --service-principal malware-
protection.guardduty.amazonaws.com
```

2. (Optional) Um den GuardDuty-initiated Malware-Scan für das Verwaltungskonto zu aktivieren, das kein delegiertes Administratorkonto ist, erstellt das Verwaltungskonto zuerst das Konto Service-linked Rollenberechtigungen für Malware Protection for EC2 explizit in seinem Konto und aktiviert dann den GuardDuty-initiated Malware-Scan vom delegierten Administratorkonto aus, ähnlich wie bei jedem anderen Mitgliedskonto.

```
aws iam create-service-linked-role --aws-service-name malware-
protection.guardduty.amazonaws.com
```

3. Sie haben das delegierte GuardDuty Administratorkonto im aktuell ausgewählten Konto festgelegt. AWS-Region Wenn Sie in einer Region ein Konto als delegiertes GuardDuty Administratorkonto festgelegt haben, muss dieses Konto in allen anderen Regionen Ihr delegiertes GuardDuty Administratorkonto sein. Wiederholen Sie den obigen Schritt für alle anderen Regionen.

Konfiguration des GuardDuty-initiated Malware-Scans für ein delegiertes Administratorkonto GuardDuty

Wählen Sie Ihre bevorzugte Zugriffsmethode, um den GuardDuty-initiated Malware-Scan für ein delegiertes GuardDuty Administratorkonto zu aktivieren oder zu deaktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/
2. Wählen Sie im Navigationsbereich Malware Protection for EC2 aus.
3. Wählen Sie auf der Seite Malware Protection for EC2 neben dem GuardDuty-initiated Malware-Scan die Option Bearbeiten aus.
4. Führen Sie eine der folgenden Aktionen aus:

   Verwenden Für alle Konten aktivieren

   - Wählen Sie Für alle Konten aktivieren. Dadurch wird der Schutzplan für alle aktiven GuardDuty Konten in Ihrer AWS Organisation aktiviert, einschließlich der neuen Konten, die der Organisation beitreten.
   - Wählen Sie Speichern.

   Verwenden Konten manuell konfigurieren

   - Um den Schutzplan nur für das Konto des delegierten GuardDuty Administratorkontos zu aktivieren, wählen Sie Konten manuell konfigurieren.
   - Wählen Sie im Abschnitt Konto für delegierte GuardDuty Administratoren (dieses Konto) die Option Aktivieren aus.
   - Wählen Sie Speichern.

API/CLI

Führen Sie den updateDetector API-Vorgang mit Ihrer eigenen regionalen Detektor-ID aus und übergeben Sie das `features` Objekt `name` als `EBS_MALWARE_PROTECTION` und `status` als`ENABLED`.

Sie können den GuardDuty-initiated Malware-Scan aktivieren, indem Sie den folgenden AWS CLI Befehl ausführen. Stellen Sie sicher, dass Sie ein gültiges *`detector ID`* Konto für delegierte GuardDuty Administratoren verwenden.

Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 /
              --account-ids 555555555555 /
              --features '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
```

Auto-enable GuardDuty-initiated Malware-Scan für alle Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um die GuardDuty-initiated Malware-Scan-Funktion für alle Mitgliedskonten zu aktivieren. Dazu gehören der delegierte Administrator, bestehende Mitgliedskonten und die neuen Konten, die der Organisation beitreten.

Console

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Stellen Sie sicher, dass Sie die Anmeldedaten für das delegierte GuardDuty Administratorkonto verwenden.

2. Führen Sie eine der folgenden Aktionen aus:

   Verwendung der Malware-Schutz für EC2 angezeigten

   1. Wählen Sie im Navigationsbereich Malware Protection for EC2 aus.
   2. Wählen Sie auf der Seite Malware Protection for EC2 im Abschnitt GuardDuty-initiated Malware-Scan die Option Bearbeiten aus.
   3. Wählen Sie Für alle Konten aktivieren. Diese Aktion aktiviert automatisch den GuardDuty-initiated Malware-Scan sowohl für bestehende als auch für neue Konten in der Organisation.
   4. Wählen Sie Speichern.

   > **Note**
   >
   > Die Aktualisierung der Konfiguration der Mitgliedskonten kann bis zu 24 Stunden dauern.

Verwendung der Konten angezeigten

1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
2. Wählen Sie auf der Seite „Konten“ vor Auto-enable „Konten per Einladung hinzufügen“ die Option „Einstellungen“ aus.
3. Wählen Sie im Fenster „Einstellungen für automatische Aktivierung verwalten“ die Option „Für alle Konten aktivieren, für die ein GuardDuty-initiated Malware-Scan durchgeführt wird“.
4. Wählen Sie auf der Seite Malware Protection for EC2 im Bereich GuardDuty-initiated Malware-Scan die Option Bearbeiten aus.
5. Wählen Sie Für alle Konten aktivieren. Diese Aktion aktiviert automatisch den GuardDuty-initiated Malware-Scan sowohl für bestehende als auch für neue Konten in der Organisation.
6. Wählen Sie Speichern.

> **Note**
>
> Die Aktualisierung der Konfiguration der Mitgliedskonten kann bis zu 24 Stunden dauern.

Verwendung der Konten angezeigten

1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
2. Wählen Sie auf der Seite „Konten“ vor Auto-enable „Konten per Einladung hinzufügen“ die Option „Einstellungen“ aus.
3. Wählen Sie im Fenster „Einstellungen für automatische Aktivierung verwalten“ die Option „Für alle Konten aktivieren, für die ein GuardDuty-initiated Malware-Scan durchgeführt wird“.
4. Wählen Sie Speichern.

Falls Sie die Option Für alle Konten aktivieren nicht verwenden können, finden Sie weitere Informationen unter Aktivieren Sie selektiv den GuardDuty-initiated Malware-Scan für Mitgliedskonten.

API/CLI

- Um den GuardDuty-initiated Malware-Scan für Ihre Mitgliedskonten selektiv zu aktivieren, rufen Sie den updateMemberDetectors API-Vorgang mit Ihrem eigenen auf. *`detector ID`*
- Das folgende Beispiel zeigt, wie Sie den GuardDuty-initiated Malware-Scan für ein einzelnes Mitgliedskonto aktivieren können. Um ein Mitgliedskonto zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

  Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
  ```

  Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.
- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Aktiviere den GuardDuty-initiated Malware-Scan für alle vorhandenen aktiven Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um den GuardDuty-initiated Malware-Scan für alle vorhandenen aktiven Mitgliedskonten in der Organisation zu aktivieren.

Um den GuardDuty-initiated Malware-Scan für alle vorhandenen aktiven Mitgliedskonten zu konfigurieren

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Melden Sie sich mit den Anmeldedaten für das delegierte GuardDuty Administratorkonto an.
2. Wählen Sie im Navigationsbereich Malware Protection for EC2 aus.
3. Im Malware Protection for EC2 können Sie den aktuellen Status der GuardDuty-initiated Malware-Scan-Konfiguration einsehen. Wählen Sie im Abschnitt Aktive Mitgliedskonten die Option Aktionen.

4. Wählen Sie im Dropdownmenü Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten.
5. Wählen Sie Speichern.

Auto-enable GuardDuty-initiated Malware-Scan für neue Mitgliedskonten

Die neu hinzugefügten Mitgliedskonten müssen aktiviert werden, GuardDuty bevor Sie die Konfiguration des GuardDuty-initiated Malware-Scans auswählen können. Die Mitgliedskonten, die auf Einladung verwaltet werden, können den GuardDuty-initiated Malware-Scan für ihre Konten manuell konfigurieren. Weitere Informationen finden Sie unter Step 3 - Accept an invitation.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um den GuardDuty-initiated Malware-Scan für neue Konten zu aktivieren, die Ihrer Organisation beitreten.

Console

Das delegierte GuardDuty Administratorkonto kann die GuardDuty-initiated Malware-Suche nach neuen Mitgliedskonten in einer Organisation aktivieren. Verwenden Sie dazu entweder die Seite Malware-Schutz für EC2 oder Konten.

Um den GuardDuty-initiated Malware-Scan für neue Mitgliedskonten automatisch zu aktivieren

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

   Stellen Sie sicher, dass Sie die Anmeldedaten für das delegierte GuardDuty Administratorkonto verwenden.
2. Führen Sie eine der folgenden Aktionen aus:
   - Verwenden der Seite „Malware-Schutz für EC2“:
     1. Wählen Sie im Navigationsbereich Malware Protection for EC2 aus.
     2. Wählen Sie auf der Seite Malware Protection for EC2 im GuardDuty-initiated Malware-Scan die Option Bearbeiten aus.
     3. Wählen Sie Konten manuell konfigurieren.
     4. Wählen Sie Automatisch für neue Mitgliedskonten aktivieren. Dieser Schritt stellt sicher, dass jedes Mal, wenn ein neues Konto Ihrer Organisation beitritt, der GuardDuty-initiated Malware-Scan automatisch für das entsprechende Konto aktiviert wird. Nur das delegierte GuardDuty Administratorkonto der Organisation kann diese Konfiguration ändern.

5. Wählen Sie Speichern.

- Verwenden der Seite Konten:

1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
2. Wählen Sie auf der Seite Konten die Auto-enable Einstellungen aus.
3. Wählen Sie im Fenster „Einstellungen für automatische Aktivierung verwalten“ im Rahmen des GuardDuty-initiated Malware-Scans die Option Für neue Konten aktivieren aus.
4. Wählen Sie Speichern.

API/CLI

- Um den GuardDuty-initiated Malware-Scan für neue Mitgliedskonten zu aktivieren oder zu deaktivieren, rufen Sie den UpdateOrganizationConfiguration API-Vorgang mit Ihrem eigenen auf. *`detector ID`*
- Das folgende Beispiel zeigt, wie Sie den GuardDuty-initiated Malware-Scan für ein einzelnes Mitgliedskonto aktivieren können. Informationen zur Deaktivierung finden Sie unter Aktivieren Sie selektiv den GuardDuty-initiated Malware-Scan für Mitgliedskonten. Wenn Sie es nicht für alle neuen Konten aktivieren möchten, die der Organisation beitreten, legen Sie die Einstellung `AutoEnable` auf `NONE` fest.

  Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

  ```
  aws guardduty update-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --AutoEnable --features '[{"Name":
   "EBS_MALWARE_PROTECTION", "AutoEnable": NEW}]'
  ```

  Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.
- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Aktivieren Sie selektiv den GuardDuty-initiated Malware-Scan für Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um den GuardDuty-initiated Malware-Scan für Mitgliedskonten selektiv zu konfigurieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/
2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
3. Überprüfen Sie auf der Seite Konten in der Spalte „GuardDuty-initiated Malware-Scan“ den Status Ihres Mitgliedskontos.
4. Wählen Sie das Konto aus, für das Sie den GuardDuty-initiated Malware-Scan konfigurieren möchten. Sie können mehrere Konten gleichzeitig auswählen.
5. Wählen Sie im Menü Schutzpläne bearbeiten die entsprechende Option für den GuardDuty-initiated Malware-Scan aus.

API/CLI

Um den GuardDuty-initiated Malware-Scan für Ihre Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren, rufen Sie den updateMemberDetectors API-Vorgang mit Ihrem eigenen auf. *detector ID*

Das folgende Beispiel zeigt, wie Sie den GuardDuty-initiated Malware-Scan für ein einzelnes Mitgliedskonto aktivieren können.

Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name": "EBS_MALWARE_PROTECTION",
 "Status": "ENABLED"}]'
```

Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Um den GuardDuty-initiated Malware-Scan für Ihre Mitgliedskonten selektiv zu aktivieren, führen Sie den updateMemberDetectors API-Vorgang mit Ihrem eigenen *detector ID* aus. Das folgende Beispiel zeigt, wie Sie den GuardDuty-initiated Malware-Scan für ein einzelnes Mitgliedskonto aktivieren können.

Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --data-sources '{"MalwareProtection":
{"ScanEc2InstanceWithFindings":{"EbsVolumes":true}}}'
```

Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Aktiviere den GuardDuty-initiated Malware-Scan für bestehende Konten in der Organisation, die per Einladung verwaltet werden

Die Service-Linked Role (SLR) von GuardDuty Malware Protection for EC2 muss in den Mitgliedskonten erstellt werden. Das Administratorkonto kann die GuardDuty-initiated Malware-Scan-Funktion in Mitgliedskonten, die nicht von verwaltet werden, nicht aktivieren. AWS Organizations

Derzeit können Sie die folgenden Schritte über die GuardDuty Konsole unter ausführen, https://console.aws.amazon.com/guardduty/ um den GuardDuty-initiated Malware-Scan für die vorhandenen Mitgliedskonten zu aktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

   Melden Sie sich mit den Anmeldeinformationen Ihres Administratorkontos an.
2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
3. Wählen Sie das Mitgliedskonto aus, für das Sie den GuardDuty-initiated Malware-Scan aktivieren möchten. Sie können mehrere Konten gleichzeitig auswählen.

4. Wählen Sie Aktionen.
5. Wählen Sie Mitglied trennen.
6. Wählen Sie im Mitgliedskonto im Navigationsbereich Malware Protection unter Schutzpläne.
7. Wählen Sie GuardDuty-initiated Malware-Scan aktivieren. GuardDuty erstellt eine Spiegelreflexkamera für das Mitgliedskonto. Weitere Informationen zu SLR finden Sie unter Service-linked Rollenberechtigungen für Malware Protection for EC2.
8. Wählen Sie in Ihrem Administratorkonto im Navigationsbereich Konten aus.
9. Wählen Sie das Mitgliedskonto aus, das der Organisation wieder hinzugefügt werden muss.
10. Wählen Sie Aktionen und dann Mitglied hinzufügen.

API/CLI

1. Verwenden Sie das Administratorkonto, um die DisassociateMembers API für die Mitgliedskonten auszuführen, die den GuardDuty-initiated Malware-Scan aktivieren möchten.
2. Verwenden Sie Ihr Mitgliedskonto, um den GuardDuty-initiated Malware-Scan aufzurufen und UpdateDetector zu aktivieren.

   Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

   ```
   aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
    --data-sources '{"MalwareProtection":{"ScanEc2InstanceWithFindings":
   {"EbsVolumes":true}}}'
   ```

3. Verwenden Sie das Administratorkonto, um die CreateMembers API auszuführen und das Mitglied wieder zur Organisation hinzuzufügen.

Aktivierung des GuardDuty-initiated Malware-Scans für ein eigenständiges Konto

Ein eigenständiges Konto entscheidet selbst, ob ein Schutzpaket AWS-Konto in einem bestimmten Bereich aktiviert oder deaktiviert werden soll AWS-Region.

Wenn Ihr Konto durch oder durch AWS Organizations die Einladungsmethode mit einem GuardDuty Administratorkonto verknüpft ist, gilt dieser Abschnitt nicht für Ihr Konto. Weitere Informationen finden Sie unter Aktivierung des GuardDuty-initiated Malware-Scans in Umgebungen mit mehreren Konten.

Nachdem Sie den GuardDuty-initiated Malware-Scan aktiviert haben, GuardDuty wird ein Malware-Scan des Amazon EBS-Volumes initiiert, das an die Amazon EC2-Instance angehängt ist, die an einem beteiligt war. GuardDuty Eine Liste der Ergebnisse, die den Malware-Scan initiieren, finden Sie unter. Ergebnisse, die den GuardDuty-initiated Malware-Scan auslösen

Wählen Sie Ihre bevorzugte Zugriffsmethode, um den GuardDuty-initiated Malware-Scan für ein eigenständiges Konto zu konfigurieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich unter Schutzpläne die Option Malware Protection for EC2 aus.
3. Im Bereich Malware Protection for EC2 wird der aktuelle Status des GuardDuty-initiated Malware-Scans für Ihr Konto aufgeführt. Wählen Sie Aktivieren, um den GuardDuty-initiated Malware-Scan in diesem Konto zu aktivieren.
4. Wählen Sie Speichern, um Ihre Auswahl zu bestätigen.

API/CLI

Führen Sie den updateDetector API-Vorgang mit Ihrer eigenen regionalen Detektor-ID aus und übergeben Sie das `dataSources` Objekt mit `EbsVolumes` set to`true`.

Sie können den GuardDuty-initiated Malware-Scan auch aktivieren, AWS CLI indem Sie den folgenden AWS CLI Befehl ausführen. Stellen Sie sicher, dass Sie Ihr eigenes gültiges Passwort verwenden*detector ID*.

Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

```
 aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features [{"Name" : "EBS_MALWARE_PROTECTION", "Status" : "ENABLED"}]'
```

Ergebnisse, die den GuardDuty-initiated Malware-Scan auslösen

Wenn verdächtiges Verhalten GuardDuty erkannt wird, das auf Malware auf einer Amazon EC2-Instance oder einem Container-Workload hindeutet, der auf einer Amazon EC2-Instance ausgeführt wird, GuardDuty wird ein Befund generiert. Wenn dieser generierte Befund zu der folgenden Ergebnisliste gehört, GuardDuty wird automatisch ein Malware-Scan auf den Amazon EBS-Volumes initiiert, die mit der Amazon EC2-Instance verbunden sind, die an dem Fund beteiligt ist. GuardDuty Wenn nach dem Scan Malware GuardDuty erkannt wird, werden auch eine oder mehrere generiert. Malware-Schutz für EC2-Suchtypen

Wenn einer der folgenden GuardDuty Ergebnisse in Ihrem Konto generiert GuardDuty wird, wird automatisch ein Malware-Scan im Amazon EBS-Volume der potenziell gefährdeten Amazon EC2-Instance initiiert.

- Backdoor:EC2/C&CActivity.B
- Backdoor:EC2/C&CActivity.B!DNS
- Backdoor:EC2/DenialOfService.Dns
- Backdoor:EC2/DenialOfService.Tcp
- Backdoor:EC2/DenialOfService.Udp
- Backdoor:EC2/DenialOfService.UdpOnTcpPorts
- Backdoor:EC2/DenialOfService.UnusualProtocol
- Backdoor:EC2/Spambot
- CryptoCurrency:EC2/BitcoinTool.B
- CryptoCurrency:EC2/BitcoinTool.B!DNS
- DefenseEvasion:Runtime/PtraceAntiDebugging
- DefenseEvasion:Runtime/SuspiciousCommand
- Execution:Runtime/MaliciousFileExecuted
- Execution:Runtime/MaliciousFileExecuted.Custom
- Execution:Runtime/SuspiciousCommand
- Execution:Runtime/SuspiciousShellCreated
- Execution:Runtime/SuspiciousTool
- Impact:EC2/AbusedDomainRequest.Reputation
- Impact:EC2/BitcoinDomainRequest.Reputation

- Impact:EC2/MaliciousDomainRequest.Reputation
- Impact:EC2/PortSweep
- Impact:EC2/SuspiciousDomainRequest.Reputation
- Impact:EC2/WinRMBruteForce (Nur ausgehend)
- PrivilegeEscalation:Runtime/ElevationToRoot
- Recon:EC2/Portscan
- Trojan:EC2/BlackholeTraffic
- Trojan:EC2/BlackholeTraffic!DNS
- Trojan:EC2/DGADomainRequest.B
- Trojan:EC2/DGADomainRequest.C!DNS
- Trojan:EC2/DNSDataExfiltration
- Trojan:EC2/DriveBySourceTraffic!DNS
- Trojan:EC2/DropPoint
- Trojan:EC2/DropPoint!DNS
- Trojan:EC2/PhishingDomainRequest!DNS
- UnauthorizedAccess:EC2/RDPBruteForce (Nur ausgehend)
- UnauthorizedAccess:EC2/SSHBruteForce (Nur ausgehend)
- UnauthorizedAccess:EC2/TorClient
- UnauthorizedAccess:EC2/TorRelay
- Backdoor:Runtime/C&CActivity.B
- Backdoor:Runtime/C&CActivity.B! DNS
- CryptoCurrency:Runtime/BitcoinTool.B
- CryptoCurrency:Runtime/BitcoinTool.B! DNS
- Execution:Runtime/NewBinaryExecuted
- Execution:Runtime/NewLibraryLoaded
- Execution:Runtime/ReverseShell
- Impact:Runtime/AbusedDomainRequest.Reputation
- Impact:Runtime/BitcoinDomainRequest.Reputation
- Impact:Runtime/CryptoMinerExecuted
- Impact:Runtime/MaliciousDomainRequest.Reputation

- Impact:Runtime/SuspiciousDomainRequest.Reputation
- PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified
- PrivilegeEscalation:Runtime/ContainerMountsHostDirectory
- PrivilegeEscalation:Runtime/DockerSocketAccessed
- PrivilegeEscalation:Runtime/RuncContainerEscape
- PrivilegeEscalation:Runtime/UserfaultfdUsage
- Trojan:Runtime/BlackholeTraffic
- Trojan:Runtime/BlackholeTraffic! DNS
- Trojan:Runtime/DropPoint
- Trojan:Runtime/DropPoint! DNS
- Trojan:Runtime/DGADomainRequest.C! DNS
- Trojan:Runtime/DriveBySourceTraffic! DNS
- Trojan:Runtime/PhishingDomainRequest! DNS
- UnauthorizedAccess:Runtime/MetadataDNSRebind

On-demand Malware-Scan in GuardDuty

On-demand Der Malware-Scan hilft Ihnen, das Vorhandensein von Malware auf Amazon Elastic Block Store (Amazon EBS) -Volumes zu erkennen, die an Ihre Amazon EC2-Instances angehängt sind. Da keine Konfiguration erforderlich ist, können Sie einen On-Demand-Malware-Scan starten, indem Sie den Amazon-Ressourcennamen (ARN) der Amazon EC2-Instance angeben, die Sie scannen möchten. Sie können einen On-Demand-Malware-Scan entweder über die GuardDuty Konsole oder die API starten. Bevor Sie einen Malware-Scan auf Abruf starten, können Sie Ihre bevorzugte Snapshot-Beibehaltung-Einstellung festlegen. Anhand der folgenden Szenarien können Sie ermitteln, wann Sie den On-demand Malware-Scan-Typ verwenden sollten GuardDuty:

- Sie möchten das Vorhandensein von Malware in Ihren Amazon EC2-Instances erkennen, ohne den GuardDuty-initiated Malware-Scan zu aktivieren.
- Sie haben den GuardDuty-initiated Malware-Scan aktiviert und ein Scan wurde automatisch gestartet. Wenn Sie einen Scan auf derselben Ressource starten möchten, nachdem Sie die empfohlene Problembehebung für den generierten Findetyp „Malware-Schutz für EC2“ befolgt haben, können Sie einen Malware-Scan auf Anforderung starten, nachdem 1 Stunde ab der Startzeit des vorherigen Scans vergangen ist.

On-demand Für den Malware-Scan ist es nicht erforderlich, dass seit dem Start des vorherigen Malware-Scans 24 Stunden vergangen sind. Eine Stunde sollte vergangen sein, bevor ein On-demand Malware-Scan auf derselben Ressource gestartet wurde. Informationen dazu, wie Sie vermeiden können, dass ein Malware-Scan auf derselben EC2-Instance dupliziert wird, finden Sie unter Re-scanning zuvor gescannte Amazon EC2-Instance.

> **Note**
>
> On-demand Der Malware-Scan ist nicht in der 30-tägigen kostenlosen Testphase mit enthalten. GuardDuty Die Nutzungskosten beziehen sich auf das gesamte Amazon-EBS-Volumen, das bei jedem Malware-Scan gescannt wurde. Weitere Informationen finden Sie unter GuardDuty Amazon-Preise. Informationen zu den Kosten der Erstellung von Amazon-EBS-Volume-Snapshots und deren Aufbewahrung finden Sie unter Amazon-EBS-Preise.

So funktioniert der On-demand Malware-Scan

Mit dem On-demand Malware-Scan können Sie eine Malware-Scan-Anfrage für Ihre Amazon EC2-Instance starten, auch wenn diese gerade verwendet wird. Nachdem Sie einen On-demand Malware-Scan gestartet haben, GuardDuty erstellt Snapshots der Amazon EBS-Volumes, die an die Amazon EC2-Instance angehängt sind, deren Amazon-Ressourcenname (ARN) für den Scan bereitgestellt wurde. Als Nächstes GuardDuty teilt er diese Snapshots mit dem. GuardDuty Dienstkonto GuardDuty erstellt verschlüsselte Replikat-EBS-Volumes aus diesen Snapshots im Dienstkonto. GuardDuty Weitere Informationen dazu, wie Amazon-EBS-Volumes gescannt werden finden Sie unter Wie werden EBS-Volumes zur Erkennung von Schadsoftware GuardDuty gescannt.

> **Note**
>
> GuardDuty erstellt die Snapshots der Daten, die zu dem Zeitpunkt, zu dem Sie einen Malware-Scan starten, bereits auf die Amazon EBS-Volumes geschrieben wurden. On-demand

Wenn Malware gefunden wird und Sie die Einstellung zur Aufbewahrung von Snapshots aktiviert haben, werden die Snapshots Ihres EBS-Volumes automatisch in Ihrem gespeichert. AWS-Konto On-demand Der Malware-Scan generiert die. Malware-Schutz für EC2-Suchtypen Wenn keine Malware

gefunden wird, werden die Snapshots Ihrer EBS-Volumes gelöscht, unabhängig von der Einstellung zur Beibehaltung von Snapshots.

GuardDuty verwendet einen globalen Tag-Schlüssel`GuardDutyExcluded`, den Sie zu Ihren Amazon EC2-Ressourcen hinzufügen und den Tag-Wert auf `true` setzen können. Diese Amazon EC2-Ressource, die über dieses Tag-Schlüssel-Wert-Paar verfügt, wird vom Malware-Scan ausgeschlossen. Beide Scantypen (GuardDuty-initiated Malware-Scan und On-demand Malware-Scan) unterstützen das globale Tag. Wenn Sie einen On-Demand-Malware-Scan auf einem Amazon EC2 starten, wird eine Scan-ID generiert. Der Scan wird jedoch mit einem `EXCLUDED_BY_SCAN_SETTINGS` Grund übersprungen. Weitere Informationen finden Sie unter Gründe für das Überspringen von Ressourcen beim Malware-Scan.

Der On-demand Malware-Scan wird gestartet in GuardDuty

Dieser Abschnitt enthält eine Liste der Voraussetzungen, bevor ein On-Demand-Malware-Scan gestartet werden kann, sowie Schritte, um den Scan auf einer Ressource zum ersten Mal zu starten.

Als GuardDuty Administratorkonto können Sie einen On-Demand-Malware-Scan im Namen Ihrer aktiven Mitgliedskonten starten, für deren Konten die folgenden Voraussetzungen festgelegt sind. Eigenständige Konten und aktive Mitgliedskonten in GuardDuty können auch einen On-Demand-Malware-Scan für ihre eigenen Amazon EC2-Instances starten.

Voraussetzungen

Bevor Sie einen On-demand Malware-Scan starten, muss Ihr Konto die folgenden Voraussetzungen erfüllen:

- GuardDuty muss in dem Bereich aktiviert sein AWS-Regionen , an dem Sie den On-Demand-Malware-Scan starten möchten.
- Stellen Sie sicher, dass der AWS verwaltete Richtlinie: AmazonGuardDutyFullAccess_v2 (empfohlen) dem IAM-Benutzer oder der IAM-Rolle angefügt ist. Sie benötigen den Zugriffsschlüssel und den geheimen Schlüssel, die dem IAM-Benutzer oder der IAM-Rolle zugeordnet sind.
- Als delegiertes GuardDuty Administratorkonto haben Sie die Möglichkeit, im Namen eines aktiven Mitgliedskontos einen On-Demand-Malware-Scan zu starten.
- Bevor Sie einen On-Demand-Malware-Scan starten, stellen Sie sicher, dass in der letzten 1 Stunde kein Scan auf derselben Ressource gestartet wurde. Andernfalls wird der Scan dedupliziert. Weitere Informationen finden Sie unter Re-scanning zuvor gescannte Amazon EC2-Instance.

- Wenn Sie ein Mitgliedskonto sind, das nicht über das verfügtService-linked Rollenberechtigungen für Malware Protection for EC2, wird beim Initiieren eines On-Demand-Malwarescans für eine Amazon EC2-Instance, die zu Ihrem Konto gehört, automatisch die SLR für Malware Protection for EC2 erstellt.

> **Important**
>
> Stellen Sie sicher, dass niemand die SLR-Berechtigungen für Malware Protection for EC2 löscht, wenn der Malware-Scan noch läuft. Dieser Malware-Scan kann entweder von GuardDuty oder bei Bedarf gestartet werden. Das Löschen der Spiegelreflexkamera verhindert, dass der Scan erfolgreich abgeschlossen wird und ein eindeutiges Scanergebnis liefert.

Starten Sie den On-demand Malware-Scan

Sie können einen On-Demand-Malware-Scan in Ihrem Konto über die GuardDuty Konsole oder mithilfe von starten AWS CLI. Sie müssen den Amazon EC2-Amazon-Ressourcennamen (ARN) angeben, für den Sie den Scan starten möchten. Die detaillierten Schritte finden Sie sowohl in der Konsole als auch in den AWS CLI API/Anweisungen im folgenden Abschnitt.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um einen On-Demand-Malware-Scan zu starten.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Starten Sie den Scan mit einer der folgenden Optionen:
   a. Verwenden Sie die Seite „Malware-Schutz für EC2“:
      i. Wählen Sie im Navigationsbereich unter Schutzpläne die Option Malware Protection for EC2 aus.
      ii. Geben Sie auf der Seite Malware Protection for EC2 die Amazon EC2-Instance ARN [1 an,] für die Sie den Scan starten möchten.
   b. Verwendung der Seite Malware-Scans:
      i. Wählen Sie im Navigationsbereich Malware-Scans.

ii. Wählen Sie On-Demand-Scan starten und geben Sie die Amazon EC2-Instance ARN [1] an, für die Sie den Scan starten möchten.

iii. Wenn es sich um einen Wiederholungs-Scan handelt, wählen Sie auf der Seite Malware-Scans eine Amazon-EC2-Instance-ID aus.

Erweitern Sie das Drop-down-Menü On-Demand-Scan starten und wählen Sie die Re-scan ausgewählte Instance aus.

3. Nachdem Sie einen Scan mit einer der beiden Methoden erfolgreich gestartet haben, wird eine Scan-ID generiert. Sie können diese Scan-ID verwenden, um den Scan-Fortschritt zu verfolgen. Weitere Informationen finden Sie unter Überwachen von Scanstatus und Ergebnissen.

API/CLI

Invoke StartMalwareScan, der den Wert `resourceArn` der Amazon EC2-Instance [1] akzeptiert, für die Sie einen On-Demand-Malware-Scan starten möchten.

```
aws guardduty start-malware-scan --resource-arn "arn:aws:ec2:us-
east-1:555555555555:instance/i-b188560f"
```

Nachdem Sie einen Scan erfolgreich gestartet haben, wird ein `StartMalwareScan` zurückgegeben. `scanId` Rufen DescribeMalwareScans Sie die Überwachung des Fortschritts des gestarteten Scans auf.

[1]Informationen zum Format Ihres Amazon-EC2-Instance-ARN finden Sie unter Amazon-Ressourcenname (ARN). Für Amazon-EC2-Instances können Sie das folgende ARN-Beispielformat verwenden, indem Sie die Werte für die Partition, Region, AWS-Konto -ID und Amazon-EC2-Instance-ID ersetzen. Informationen zur Länge Ihrer Instance-ID finden Sie unter Ressourcen-IDs.

```
arn:aws:ec2:us-east-1:555555555555:instance/i-b188560f
```

AWS Organizations Service Control-Richtlinie — Zugriff verweigert

Mithilfe der Service Control Policies (SCPs) in AWS Organizations kann das delegierte GuardDuty Administratorkonto Berechtigungen einschränken und Aktionen wie das Initiieren eines On-Demand-Malware-Scans für die Amazon EC2-Instance verweigern, die Ihren Konten gehört.

Wenn Sie als GuardDuty Mitgliedskonto einen On-Demand-Malware-Scan für Ihre Amazon EC2-Instances starten, erhalten Sie möglicherweise eine Fehlermeldung. Sie können sich mit dem Verwaltungskonto verbinden, um zu erfahren, warum ein SCP für Ihr Mitgliedskonto eingerichtet wurde. Weitere Informationen zu SCP-Auswirkungen auf Berechtigungen.

Re-scanning zuvor gescannte Amazon EC2-Instance

Unabhängig davon, ob ein Scan auf Abruf erfolgt GuardDuty-initiated oder gestartet wird, können Sie einen neuen On-Demand-Malware-Scan auf derselben Amazon EC2-Instance starten, und zwar innerhalb einer Stunde ab der Startzeit des vorherigen Malware-Scans. Wenn der neue Malware-Scan innerhalb von 1 Stunde nach Beginn des vorherigen Malware-Scans gestartet wird, führt Ihre Anfrage zu dem folgenden Fehler, und für diese Anfrage wird keine Scan-ID generiert.

```
A scan was started on this resource recently. You can request a scan on the same resource one hour after the previous scan start time.
```

Die Schritte zum erneuten Scannen der Instanz bleiben dieselben wie beim ersten Starten eines On-Demand-Malware-Scans. Informationen zu den Schritten finden Sie unterStarten Sie den On-demand Malware-Scan.

Informationen zum Verfolgen des Status der Malware-Scans finden Sie unter Überwachung des Scanstatus und der Ergebnisse in Malware Protection for EC2.

Überwachung des Scanstatus und der Ergebnisse in Malware Protection for EC2

Nachdem ein Malware-Scan auf einer Amazon EC2-Instance initiiert wurde, werden die Status- und Ergebnisfelder automatisch GuardDuty bereitgestellt. Sie können den Status anhand von Übergängen überwachen und sehen, ob Malware erkannt wurde. Die folgende Tabelle enthält die möglichen Werte, die dem Malware-Scan zugeordnet sind.

Mögliche Werte
`Running`, `Completed` `Skipped`, oder `Failed`
`Clean` oder `Infected`

Mögliche Werte
`GuardDuty initiated` oder `On demand`

*Das Scan-Ergebnis wird nur ausgefüllt, wenn der Scanstatus lautet. `Completed` Das Scanergebnis `Infected` bedeutet, dass das Vorhandensein von Malware GuardDuty erkannt wurde.

Die Scan-Ergebnisse für jeden Malware-Scan werden 90 Tage aufbewahrt. Wählen Sie Ihre bevorzugte Zugriffsmethode, um den Status Ihres Malware-Scans zu verfolgen.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich EC2-Malware-Scans aus.
3. Sie können die Malware-Scans anhand der folgenden Eigenschaften filtern, die in der Filter-Suchleiste verfügbar sind.
   - Scan-ID — Eindeutige Kennung, die dem EC2-Malware-Scan zugeordnet ist.
   - Konto-ID — AWS-Konto ID, mit der der Malware-Scan initiiert wurde.
   - EC2-Instance-ARN — Amazon-Ressourcenname (ARN), der der Amazon EC2-Instance zugeordnet ist, die dem Scan zugeordnet ist.
   - Scanstatus — Der Scanstatus des EBS-Volumes, z. B. Wird ausgeführt, Übersprungen und Abgeschlossen
   - Scan-Typ — Gibt an, ob es sich um einen On-demand Malware-Scan oder einen GuardDuty-initiated Malware-Scan handelt.

API/CLI

- Nachdem der Malware-Scan ein Scan-Ergebnis erhalten hat, verwenden Sie diese Option, DescribeMalwareScans um die Malware-Scans auf der Grundlage von `EC2_INSTANCE_ARN`SCAN_ID,`ACCOUNT_ID`, `SCAN_TYPE` `GUARDDUTY_FINDING_ID`SCAN_STATUS, und zu filtern`SCAN_START_TIME`.

Die GUARDDUTY_FINDING_ID Filterkriterien sind verfügbar, wenn der GuardDuty initiiert SCAN_TYPE wird.

- Sie können das Beispiel *filter-criteria* im folgenden Befehl ändern. Gegenwärtig können Sie auf der Grundlage von jeweils einem CriterionKey filtern. Die Optionen für CriterionKey sind EC2_INSTANCE_ARN, SCAN_ID, ACCOUNT_ID, SCAN_TYPE, GUARDDUTY_FINDING_ID, SCAN_STATUS und SCAN_START_TIME.

  Sie können die *max-results* (bis zu 50) und die ändern*sort-criteria*. Der AttributeName ist verpflichtend und muss scanStartTime sein.

  Im folgenden Beispiel *red* sind die Werte in Platzhalter. Ersetzen Sie sie durch die für Ihr Konto geeigneten Werte. Ersetzen Sie beispielsweise das Beispiel durch Ihr detector-id *60b87779336485625 54d637e0e4bb3b2* eigenes gültiges Beispieldetector-id. Wenn Sie dasselbe CriterionKey wie unten verwenden, stellen Sie sicher, dass Sie das Beispiel EqualsValue durch Ihr eigenes gültiges Beispiel ersetzen AWS *scan-id*.

  ```
  aws guardduty describe-malware-scans --detector-
  id 60b87779336485625 54d637e0e4bb3b2 --max-results 1 --sort-criteria
   '{"AttributeName": "scanStartTime", "OrderBy": "DESC"}' --filter-criteria
   '{"FilterCriterion":[{"CriterionKey":"SCAN_ID", "FilterCondition":
  {"EqualsValue":"123456789012"}}] }'
  ```

- Die Antwort auf diesen Befehl zeigt maximal eine Erkenntnis mit Details zur betroffenen Ressource und zu den Malware-Erkenntnissen (wenn Infected) an.

GuardDuty Dienstkonten von AWS-Region

Wenn ein Snapshot erstellt und mit einem GuardDuty Dienstkonto geteilt wird, wird ein neues Ereignis in Ihren CloudTrail Protokollen erstellt. Dieses Ereignis gibt das entsprechende snapshotId Und userId (GuardDuty Dienstkonto dafür AWS-Region) an. Weitere Informationen finden Sie unter Wie werden EBS-Volumes zur Erkennung von Schadsoftware GuardDuty gescannt.

Das folgende Beispiel ist ein Ausschnitt aus einem CloudTrail Ereignis, das den Anforderungstext für die ModifySnapshotAttribute Anfrage zeigt:

```
"requestParameters": {
        "snapshotId": "snap-1234567890abcdef0",
        "createVolumePermission": {
```

```
            "add": {
                "items": [
                    {
                        "userId": "111122223333"
                    }
                ]
            }
        },
        "attributeType": "CREATE_VOLUME_PERMISSION"
    }
```

Die folgende Tabelle zeigt die GuardDuty Dienstkonten für jede Region. Das `userId` ist das GuardDuty Dienstkonto und hängt von der ausgewählten Region ab.

AWS-Region	Regionscode	GuardDuty Dienstkonto-ID (**`userId`**)
USA Ost (Nord-Virginia)	us-east-1	652050842985
USA Ost (Ohio)	us-east-2	178123968615
USA West (Nordkali fornien)	us-west-1	669213148797
USA West (Oregon)	us-west-2	447226417196
Asien-Pazifik (Mumbai)	ap-south-1	913179291432
Asien-Pazifik (Osaka)	ap-northeast-3	089661699081
Asien-Pazifik (Seoul)	ap-northeast-2	039163547507
Asien-Pazifik (Tokio)	ap-northeast-1	874749492622
Asien-Pazifik (Singapur)	ap-southeast-1	247460962669
Asien-Pazifik (Sydney)	ap-southeast-2	124839743349
Kanada (Zentral)	ca-central-1	175877067165
Kanada West (Calgary)	ca-west-1	894794104037
Europa (Frankfurt)	eu-central-1	002294850712

AWS-Region	Regionscode	GuardDuty Dienstkonto-ID (**`userId`**)
Europa (Irland)	eu-west-1	283769539786
Europa (London)	eu-west-2	310125036783
Europa (Paris)	eu-west-3	866607715269
Europa (Stockholm)	eu-north-1	693780578038
China (Peking)	cn-north-1	448721096076
China (Ningxia)	cn-northwest-1	480864352451
Südamerika (São Paulo)	sa-east-1	546914126324
Asien-Pazifik (Hyderabad) (Opt-in)	ap-south-2	682251015962
Asien-Pazifik (Melbourne) (Opt-in)	ap-southeast-4	353488359550
Asien-Pazifik (Malaysia) () Opt-in	ap-southeast-5	009160069308
Asien-Pazifik (Thailand) () Opt-in	ap-southeast-7	941377115582
Europa (Spanien) (Opt-in)	eu-south-2	936182149045
Europa (Zürich) (Opt-in)	eu-central-2	867642063380
Israel (Tel Aviv) (Opt-in)	il-central-1	619233833001
Europa (Mailand) (Opt-in)	eu-south-1	977238331021
Asien-Pazifik (Hongkong) (Opt-in)	ap-east-1	249472122084
Naher Osten (Bahrain) (Opt-in)	me-south-1	404001805210

AWS-Region	Regionscode	GuardDuty Dienstkonto-ID (**`userId`**)
Afrika (Kapstadt) (Opt-in)	af-south-1	957664736811
Asien-Pazifik (Jakarta) (Opt-in)	ap-southeast-3	452118225523
Naher Osten (VAE) (Opt-in)	me-central-1	828603743433
Mexiko (Zentral) () Opt-in	mx-central-1	557690616787
Asien-Pazifik (Taipeh)	ap-east-2	863518437308
Asien-Pazifik (Neuseeland)	ap-southeast-6	686255982852
AWS GovCloud (US-East)	us-gov-east-1	226283551151
AWS GovCloud (US-West)	us-gov-west-1	226300430612

Kontingente im Malware-Schutz für EC2

Dieser Abschnitt enthält die Kontingente im Zusammenhang mit der Verwendung von Malware Protection for EC2. Informationen zu den damit verbundenen Kontingenten finden Sie unterGuardDuty Kontingente. GuardDuty

Die folgende Tabelle enthält die Standardverfügbarkeit verschiedener Ressourcen, wenn Sie Malware Protection for EC2 verwenden.

Scope	Standard	Kommentare
Extraktion und Analyse von Daten in komprimierten oder archivierten Dateien	5	Die maximale Anzahl von verschachtelten Ebenen, die in einer archivierten Datei zulässig sind.

Scope	Standard	Kommentare
Anzahl der Dateien in einer archivierten Datei	1000	Die maximale Anzahl an Dateien, die in einem Archiv gescannt werden können. Diese Anzahl ist die Summe der aus dem Archiv extrahier ten Dateien und der Anzahl der aus allen verschachtelten Archiven extrahierten Dateien.
Anzahl der Bedrohungen	32	Die maximale Anzahl von Bedrohungen, die Sie im Ergebnisbereich einsehen können. GuardDuty Malware Protection for EC2 hat möglicherweise mehr Bedrohungsnamen erkannt. Wenn die Anzahl der erkannten Bedrohungsnamen höher als der Standardwert ist, können Sie die JSON-Deta ils anzeigen, indem Sie im Detailbereich der GuardDuty Konsole die Such-ID unter dem Suchnamen auswählen.
Anzahl der Dateien pro erkannter Bedrohung	5	Die maximale Anzahl identifiz ierter Dateien pro erkannter Bedrohung. Wenn beispiels weise 10 Dateien GuardDuty erkannt werden, die einer einzelnen Bedrohung zugeordnet sind, zeigt die Bedrohung maximal 5 Dateien an.

Scope	Standard	Kommentare
EBS-Volumes pro Scan pro Instance	11	Die maximale Anzahl von EBS-Volumes, die pro GuardDuty EC2-Instance gescannt werden können. Wenn mehr als 11 EBS-Volumes gescannt werden müssen, sortiert GuardDuty Malware Protection for EC2 diese `deviceName` alphabetisch und wählt die ersten 11 EBS-Volumes aus.
EBS-Volume-Größe	2048 GB	In Verbindung mit einer Amazon EC2-Instance und einem Container-Workload kann GuardDuty Malware Protection for EC2 jedes Amazon EBS-Volume mit einer Größe von bis zu 2048 GB scannen. Dieses Kontingent gilt für alle, AWS-Region in denen die Unterstützung für Malware Protection for EC2 verfügbar ist.

Scope	Standard	Kommentare
Unterstützte Dateitypen	GuardDuty Malware Protection for EC2 kann die folgenden Dateisystemtypen scannen: • Dateisystem mit neuer Technologie (NTFS) • X-Dateisystem (XFS) • Zweites erweitertes Dateisystem (ext2) • Viertes erweitertes Dateisystem (ext4) • Dateisystem mit Dateizuordnungstabelle (FAT) • Virtuelles Dateisystem mit Dateizuordnungstabelle (VFAT)	N/A.
Scan-Optionen-Tags	50	Die maximale Anzahl von Ressourcen-Tags, die Sie hinzufügen können, um die Einstellungen Ihrer Malware-Scan-Optionen anzupassen. Weitere Informationen finden Sie unter Scan-Optionen mit benutzerdefinierten Tags.
Aufbewahrungszeitraum für Ergebnisse	90	Die maximale Anzahl von Tagen, für die ein GuardDuty Ergebnis gespeichert wird. Die neuesten Informationen finden Sie unter GuardDuty Amazon-Kontingente.

Scope	Standard	Kommentare
Beibehaltungszeitraum für Malware-Scans	90	Die maximale Anzahl von Tagen, für die GuardDuty Malware Protection for EC2 den Verlauf eines Scans speichert. Weitere Informationen zum Anzeigen der letzten Malware-Scans finden Sie unter Überwachung des Scanstatus und der Ergebnisse in Malware Protection for EC2.
Transaktionen pro Sekunde (TPS) für den Malware-Scan On-demand	1	Die Anzahl der On-demand Malware-Scan-Anfragen, die pro Sekunde in jeder Region initiiert werden können.
Burst-Limit für On-demand Malware-Scans	1	Die Anzahl gleichzeitiger Anfragen zur Suche nach On-demand Schadsoftware, die pro Sekunde in jeder Region initiiert werden können.

GuardDuty Malware-Schutz für S3

Malware Protection for S3 hilft Ihnen dabei, potenzielles Vorhandensein von Malware zu erkennen, indem neu hochgeladene Objekte in Ihren ausgewählten Amazon Simple Storage Service (Amazon S3) -Bucket gescannt werden. Wenn ein S3-Objekt oder eine neue Version eines vorhandenen S3-Objekts in den ausgewählten Bucket hochgeladen wird, wird GuardDuty automatisch ein Malware-Scan gestartet.

Malware-Schutz für S3 — Überblick und Demo

Zwei Ansätze zur Aktivierung von Malware Protection für S3

Sie können Malware Protection for S3 aktivieren, wenn AWS-Konto Sie den GuardDuty Dienst aktivieren und Malware Protection for S3 als Teil der GuardDuty Gesamterfahrung verwenden, oder wenn Sie die Funktion Malware Protection for S3 eigenständig verwenden möchten, ohne den GuardDuty Dienst zu aktivieren. Wenn Sie Malware Protection for S3 eigenständig aktivieren, wird in der GuardDuty Dokumentation darauf hingewiesen, dass Malware Protection for S3 als eigenständige Funktion verwendet wird.

Überlegungen zur eigenständigen Verwendung von Malware Protection for S3

- GuardDuty Sicherheitserkenntnisse — Die Detector-ID ist eine eindeutige Kennung, die Ihrem Konto in einer Region zugeordnet ist. Wenn Sie die Aktivierung GuardDuty in einer oder mehreren Regionen in einem Konto vornehmen, wird für dieses Konto in jeder Region, in der Sie die Aktivierung vornehmen, automatisch eine Melder-ID erstellt GuardDuty. Weitere Informationen finden Sie im Konzepte und Schlüsselbegriffe bei Amazon GuardDuty Dokument unter Detektor.

  Wenn Sie Malware Protection for S3 unabhängig in einem Konto aktivieren, ist diesem Konto keine Detektor-ID zugeordnet. Dies wirkt sich darauf aus, welche GuardDuty Funktionen Ihnen möglicherweise zur Verfügung stehen. Wenn beispielsweise ein S3-Malware-Scan das Vorhandensein von Malware erkennt, wird in Ihrem System kein GuardDuty Ergebnis generiert, AWS-Konto da alle GuardDuty Ergebnisse mit einer Detektor-ID verknüpft sind.
- Überprüfung, ob das gescannte Objekt bösartig ist — Standardmäßig werden die Malware-Scan-Ergebnisse in Ihrem standardmäßigen EventBridge Amazon-Event-Bus und einem CloudWatch Amazon-Namespace GuardDuty veröffentlicht. Wenn Sie das Tagging bei der Aktivierung von Malware Protection for S3 für einen Bucket aktivieren, erhält das gescannte S3-Objekt ein Tag, das das Scanergebnis erwähnt. Weitere Informationen über das Markieren mit Tags finden Sie unter Optionales Markieren von Objekten auf der Grundlage des Scanergebnisses.

Allgemeine Überlegungen zur Aktivierung von Malware Protection for S3

Die folgenden allgemeinen Überlegungen gelten unabhängig davon, ob Sie Malware Protection for S3 unabhängig oder als Teil der GuardDuty Erfahrung verwenden:

- Sie können Malware Protection for S3 für einen Amazon S3 S3-Bucket aktivieren, der zu Ihrem eigenen Konto gehört. Als delegiertes GuardDuty Administratorkonto können Sie diese Funktion nicht in einem Amazon S3 S3-Bucket aktivieren, der zu einem Mitgliedskonto gehört.
- Sie können diese Funktion in den S3-Buckets aktivieren, die zu derselben Region gehören, die derzeit in der GuardDuty Konsole ausgewählt ist. GuardDuty unterstützt die Aktivierung dieser Funktion in regionsübergreifenden S3-Buckets nicht.
- Als delegiertes GuardDuty Administratorkonto erhalten Sie jedes Mal eine EventBridge Amazon-Benachrichtigung, wenn ein S3-Bucket geändert wird, den Status eines geschützten Buckets anzeigen und verstehen eines der Mitgliedskonten Ihrer Organisation für diese Funktion konfiguriert hat.

Inhalt

- Preise und Nutzungskosten für Malware Protection for S3
- Wie funktioniert Malware Protection for S3?
- Funktionen des Malware-Schutzes für S3
- (Optional) Starten Sie eigenständig mit GuardDuty Malware Protection for S3 (nur Konsole)
- Konfiguration des Malware-Schutzes für S3 für Ihren Bucket
- Schritte nach der Aktivierung von Malware Protection for S3
- On-demand S3-Malware-Scan GuardDuty
- Verwenden von tagbasierter Zugriffskontrolle (TBAC) mit Malware Protection for S3
- Status eines geschützten Buckets anzeigen und verstehen
- Überwachung von S3-Objektscans in Malware Protection for S3
- Fehlerbehebung
- Malware-Schutzplan für einen geschützten Bucket bearbeiten
- Malware-Schutz für S3 für einen geschützten Bucket deaktivieren
- Unterstützbarkeit der Amazon S3 S3-Funktionen
- Kontingente im Malware-Schutz für S3

Preise und Nutzungskosten für Malware Protection for S3

Die Preisgestaltung von Malware Protection for S3 unterscheidet sich von denen anderer Schutzpläne in GuardDuty. Während die meisten GuardDuty Schutzpläne auf eine kostenlose 30-Tage-Testversion folgen, beinhaltet Malware Protection for S3 ein kostenloses Kontingent. AWS Informationen zu den GuardDuty Preisen finden Sie unterPreisgestaltung in GuardDuty.

In der folgenden Liste sind die mit der Nutzung von Malware Protection for S3 verbundenen Kosten aufgeführt.

Kostenloses Kontingent (Kosten für das Scannen)

> Jeder AWS-Konto erhält ein kostenloses Kontingent, das die Nutzung bis zu einem bestimmten Limit pro Monat für jede Region beinhaltet. Jeder AWS-Konto erhält ein kostenloses monatliches Nutzungskontingent für die Nutzung von bis zu 1.000 Anfragen und 1 GB gescannter Daten. Wenn Ihre Nutzung das angegebene Limit überschreitet, fallen für Sie die Nutzungskosten für das Überschreitungslimit an. Vollständige Preisinformationen finden Sie unter Preise für GuardDuty Schutzpläne.

> **Important**
>
> On-demand Das Scannen ist nicht im kostenlosen Kontingent enthalten.

Informationen zu den Nutzungskosten nach der Aktivierung von Malware Protection for S3 finden Sie unterÜberprüfung der Nutzungskosten für Malware Protection for S3.

Kosten für die Nutzung von S3 Object Tagging

Wenn Sie den Malware-Schutz für S3 aktivieren, ist es optional, das Tagging für Ihre gescannten S3-Objekte zu aktivieren. Wenn Sie sich dafür entscheiden, S3 Object Tagging zu aktivieren, fallen damit Nutzungskosten an. Weitere Informationen zu den Kosten finden Sie auf der Amazon S3 S3-Preisseite unter dem Tab Management & Insights.

Die Nutzungskosten für S3 Object Tagging sind nicht im kostenlosen Kontingent enthalten.

Amazon S3 S3-APIs — GET und PUT Nutzungskosten

Es fallen Nutzungskosten an, wenn die Amazon S3 S3-APIs auf der Grundlage der IAM-Rolle GuardDuty ausgeführt werden. Wenn Sie beispielsweise die IAM-Rolle übernommen haben, GuardDuty wird die `PutObject` API ausgeführt, um das Testobjekt zu Ihrem ausgewählten Bucket hinzuzufügen. Dies hilft bei der GuardDuty Beurteilung des aktivierten Status der Funktion.

Informationen zu den Preisen für S3-API-Aufrufe in Ihrem AWS-Region finden Sie unter Anfragen und Datenabrufe auf der Amazon S3 S3-Preisseite unter dem Tab Speicher und Anfragen.

Die Nutzungskosten für Amazon S3 S3-APIs sind nicht im kostenlosen Kontingent enthalten.

EventBridge Kosten für verwaltete Regeln

GuardDuty verwendet eine EventBridge verwaltete Regel, um zu erkennen, wann neue Objekte in Ihre geschützten Buckets hochgeladen werden. Es fallen Kosten für die Amazon S3 S3-Opt-In-Ereignisse an, die von aufgenommen wurden. EventBridge Es fallen keine Kosten für die Lieferung von Veranstaltungen an. Informationen zu EventBridge-Preisen finden Sie unter EventBridge -Preise.

EventBridge Die Kosten für verwaltete Regeln sind nicht im kostenlosen Kontingent enthalten.

Überprüfung der Nutzungskosten für Malware Protection for S3

Für Ihr Konto fallen Nutzungskosten an, wenn Sie Malware Protection for S3 über das spezifische Limit im Rahmen des kostenlosen Kontingents hinaus verwenden. Informationen zum kostenlosen Kontingent finden Sie unter. Preise und Nutzungskosten für Malware Protection for S3 Beachten Sie, dass das kostenlose Kontingent nicht für das On-Demand-Objektscanning von Malware Protection for S3 gilt.

Die GuardDuty Konsole unterstützt nicht die Überprüfung der Nutzungskosten für Malware Protection for S3. Um die Nutzungskosten anzuzeigen, navigieren Sie in der https://console.aws.amazon.com/costmanagement/Konsole zu Cost Explorer. Informationen zur AWS-Konto Abrechnung finden Sie im AWS Billing Benutzerhandbuch.

Informationen zu den geschätzten Nutzungskosten in GuardDuty finden Sie unterÜberwachung der Nutzung und Schätzung der Kosten.

Wie funktioniert Malware Protection for S3?

In diesem Abschnitt werden die Komponenten von Malware Protection for S3 beschrieben, wie es funktioniert, nachdem Sie es für einen S3-Bucket aktiviert haben, und wie Sie den Status und das Ergebnis des Malware-Scans überprüfen können.

-Übersicht

Sie können Malware Protection for S3 für einen Amazon S3 S3-Bucket aktivieren, der Ihnen gehört AWS-Konto. GuardDutybietet Ihnen die Flexibilität, diese Funktion für Ihren gesamten Bucket zu aktivieren oder den Umfang des Malware-Scans auf bestimmte Objektpräfixe zu beschränken. Dabei wird der Inhalt jedes hochgeladenen Objekts GuardDuty gescannt, das mit einem der ausgewählten Präfixe beginnt. Sie können bis zu 5 Präfixe hinzufügen. Wenn Sie die Funktion für einen S3-Bucket aktivieren, wird dieser Bucket als geschützter Bucket bezeichnet.

IAM-Rollenberechtigungen

Malware Protection for S3 verwendet eine IAM-Rolle, die es GuardDuty ermöglicht, die Malware-Scanaktionen in Ihrem Namen durchzuführen. Zu diesen Aktionen gehören die Benachrichtigung über die neu hochgeladenen Objekte in Ihrem ausgewählten Bucket, das Scannen dieser Objekte und optional das Hinzufügen von Tags zu Ihren gescannten Objekten. Dies ist eine Voraussetzung für die Konfiguration Ihres S3-Buckets mit dieser Funktion.

Sie haben die Möglichkeit, entweder eine bestehende IAM-Rolle zu aktualisieren oder zu diesem Zweck eine neue Rolle zu erstellen. Wenn Sie Malware Protection for S3 für mehr als einen Bucket aktivieren, können Sie die bestehende IAM-Rolle nach Bedarf so aktualisieren, dass sie den anderen Bucket-Namen enthält. Weitere Informationen finden Sie unter IAM-Rollenrichtlinie erstellen oder aktualisieren.

Optionales Markieren von Objekten auf der Grundlage des Scanergebnisses

Wenn Sie Malware Protection for S3 für Ihren Bucket aktivieren, gibt es einen optionalen Schritt, um das Tagging für gescannte S3-Objekte zu aktivieren. Die IAM-Rolle beinhaltet bereits die Erlaubnis, Ihrem Objekt nach dem Scan Tags hinzuzufügen. Es GuardDuty werden jedoch nur Tags hinzugefügt, wenn Sie diese Option bei der Einrichtung aktivieren.

Sie müssen diese Option aktivieren, bevor ein Objekt hochgeladen wird. GuardDuty Fügt nach Abschluss des Scans dem gescannten S3-Objekt ein vordefiniertes Tag mit dem folgenden Schlüssel/Wert-Paar hinzu:

`GuardDutyMalwareScanStatus:`*`Potential scan result`*

Zu den möglichen Tagwerten für das Scanergebnis gehören`NO_THREATS_FOUND`,`THREATS_FOUND`, `UNSUPPORTEDACCESS_DENIED`, und. `FAILED` Weitere Informationen zu diesen Werten finden Sie unterthe section called “Status des potenziellen Scans und Status der Ergebnisse des S3-Objekts”.

Die Aktivierung von Tagging ist eine der Möglichkeiten, mehr über das Ergebnis des S3-Objektscans zu erfahren. Sie können diese Tags außerdem verwenden, um eine S3-Ressourcenrichtlinie für die tagbasierte Zugriffskontrolle (TBAC) hinzuzufügen, sodass Sie Maßnahmen gegen die potenziell schädlichen Objekte ergreifen können. Weitere Informationen finden Sie unter TBAC zur S3-Bucket-Ressource hinzufügen.

Wir empfehlen Ihnen, das Tagging bei der Konfiguration von Malware Protection for S3 für Ihren Bucket zu aktivieren. Wenn Sie das Tagging aktivieren, nachdem ein Objekt hochgeladen wurde und möglicherweise der Scan gestartet wurde, GuardDuty können dem gescannten Objekt keine Tags hinzugefügt werden. Informationen zu den damit verbundenen Kosten für das S3-Objekt-Tagging finden Sie unter. Preise und Nutzungskosten für Malware Protection for S3

Vorgang, nachdem Sie Malware Protection for S3 für einen Bucket aktiviert haben

Nachdem Sie Malware Protection for S3 aktiviert haben, wird eine Ressource für den Malware-Schutzplan exklusiv für den ausgewählten S3-Bucket erstellt. Diese Ressource ist mit einer Paket-ID für den Malware-Schutz verknüpft, einer eindeutigen Kennung für Ihre geschützte Ressource. Mithilfe einer der IAM-Berechtigungen wird GuardDuty anschließend eine EventBridge verwaltete Regel mit dem Namen erstellt und verwaltet. `DO-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*`

Wie GuardDuty geht man mit Ihren Daten um — Leitplanken für den Datenschutz

Malware Protection for S3 hört sich die EventBridge Amazon-Benachrichtigungen an. Wenn ein Objekt in den ausgewählten Bucket oder eines der Präfixe hochgeladen wird, wird dieses Objekt mithilfe von aus dem S3-Bucket GuardDuty heruntergeladen AWS PrivateLinkund anschließend in einer isolierten Umgebung in derselben Region gelesen, entschlüsselt und gescannt. Die Scanumgebung läuft in einer gesperrten Virtual Private Cloud (VPC) ohne Internetzugang. Die VPC ist an eine DNS-Firewall-Regelgruppe angehängt, die nur die Kommunikation mit den Domänen auf der Zulassungsliste zulässt, die Eigentümer ist. AWS Speichert das heruntergeladene S3-Objekt für die Dauer des Scans GuardDuty vorübergehend in der mit AWS Key Management Service ()AWS KMS -Schlüsseln verschlüsselten Scanumgebung.

> **Note**
>
> Standardmäßig initiieren alle Amazon S3 S3-APIs, die im Amazon S3 S3-Benutzerhandbuch unter dem Typ Object Created Event aufgeführt sind, den Malware Protection for S3-Scan. Zu diesen Ereignistypen gehören PutObjectPOST-Objekt und CompleteMultipartUpload. CopyObject

Informationen zur Methode zur GuardDuty Malware-Erkennung und zu den verwendeten Scan-Engines finden Sie unterGuardDuty Scan-Engine zur Malware-Erkennung.

Nach Abschluss des Malware-Scans GuardDuty werden die Scan-Metadaten mit dem Scanstatus verarbeitet und anschließend die heruntergeladene Kopie des Objekts gelöscht.

GuardDuty reinigt die Scanumgebung jedes Mal, bevor ein neuer Scan beginnt. GuardDuty verwendet eine bedingte Autorisierung für den Benutzerzugriff auf die Scanumgebung, und jede Zugriffsanfrage wird geprüft, genehmigt und geprüft.

Status und Ergebnis des S3-Objektscans werden überprüft

GuardDuty veröffentlicht das Ergebnisereignis des S3-Objektscans im EventBridge Amazon-Standardereignisbus. GuardDuty sendet auch die Scan-Metriken wie die Anzahl der gescannten Objekte und die Anzahl der gescannten Byte an Amazon CloudWatch. Wenn Sie Tagging aktiviert haben, GuardDuty werden das vordefinierte Tag `GuardDutyMalwareScanStatus` und ein potenzielles Scanergebnis als Tag-Wert hinzugefügt.

> **Important**
>
> GuardDuty verwendet die Zustellung mindestens einmal, was bedeutet, dass Sie möglicherweise mehrere Scanergebnisse für dasselbe Objekt erhalten. Wir empfehlen, Ihre Anwendungen so zu gestalten, dass doppelte Ergebnisse verarbeitet werden. Für jedes gescannte Objekt wird Ihnen nur einmal eine Rechnung gestellt.

Weitere Informationen finden Sie unter Überwachung von S3-Objektscans in Malware Protection for S3.

Überprüfung der generierten Ergebnisse

Die Überprüfung der Ergebnisse hängt davon ab, ob Sie Malware Protection for S3 mit verwenden oder nicht GuardDuty. Betrachten Sie folgende Szenarien:

Verwenden Sie den Malware-Schutz für S3, wenn Sie den GuardDuty Dienst aktiviert haben (Detektor-ID)

Wenn der Malware-Scan eine potenziell schädliche Datei in einem S3-Objekt erkennt, GuardDuty wird ein entsprechender Befund generiert. Sie können sich die Details des Befundes ansehen und die empfohlenen Schritte anwenden, um das Ergebnis möglicherweise zu beheben. Je nach Häufigkeit Ihrer Exportergebnisse wird das generierte Ergebnis in einen S3-Bucket und einen EventBridge Event-Bus exportiert.

Hinweise zu dem Befundtyp, der generiert werden würde, finden Sie unterSuchtyp „Malware-Schutz für S3“.

Verwendung von Malware Protection for S3 als eigenständige Funktion (keine Detektor-ID)

GuardDuty kann keine Ergebnisse generieren, da keine zugehörige Detektor-ID vorhanden ist. Um den Status des S3-Objekt-Malware-Scans zu erfahren, können Sie sich das Scanergebnis

ansehen, das GuardDuty automatisch in Ihrem Standard-Event-Bus veröffentlicht wird. Sie können sich auch die CloudWatch Metriken ansehen, um die Anzahl der Objekte und Byte einzuschätzen, die GuardDuty versucht haben, zu scannen. Sie können CloudWatch Alarme einrichten, um über die Scanergebnisse informiert zu werden. Wenn Sie S3 Object Tagging aktiviert haben, können Sie auch den Status des Malware-Scans einsehen, indem Sie das S3-Objekt auf den `GuardDutyMalwareScanStatus` Tag-Schlüssel und den Tag-Wert für das Scanergebnis überprüfen.

Informationen zum Status und zum Ergebnis des S3-Objektscans finden Sie unterÜberwachung von S3-Objektscans in Malware Protection for S3.

Funktionen des Malware-Schutzes für S3

Die folgende Liste bietet einen Überblick darüber, was Sie erwarten oder tun können, nachdem Sie Malware Protection for S3 für Ihren Bucket aktiviert haben:

- Wählen Sie aus, was gescannt werden soll — Dateien werden beim Hochladen auf alle oder bestimmte Präfixe (bis zu 5) gescannt, die Ihrem ausgewählten S3-Bucket zugeordnet sind.
- Automatische Scans hochgeladener Objekte — Sobald Sie Malware Protection for S3 für einen Bucket aktiviert haben, GuardDuty wird automatisch ein Scan gestartet, um potenzielle Malware in einem neu hochgeladenen Objekt zu erkennen.
- On-demand Scans — Sie können Scans für vorhandene Objekte starten oder zuvor gescannte Objekte erneut scannen. Weitere Informationen finden Sie unter On-demand S3-Malware-Scan GuardDuty.
- Aktivierung über die Konsole, mithilfe von API/AWS CLI, oder CloudFormation — Wählen Sie eine bevorzugte Methode, um Malware Protection for S3 zu aktivieren.

  Sie können den Malware-Schutz für S3 aktivieren, indem Sie Infrastructure-as-Code-Plattformen (IaC) wie Terraform verwenden. Weitere Informationen finden Sie unter Ressource:. `aws_guardduty_malware_protection_plan`
- Unterstützte Dateiformate, Malware Protection for S3-Kontingente und Amazon S3 S3-Funktionen — Malware Protection for S3 unterstützt alle Dateiformate, die Sie in einen S3-Bucket hochladen können. Wenn die hochgeladene Datei kennwortgeschützt GuardDuty ist und das Vorhandensein eines Kennwortschutzes für den Typ der hochgeladenen Datei erkennen kann, GuardDuty wird versucht, den Originalinhalt mit gängigen Passwörtern zu scannen. Wenn das Passwort fehlschlägt, wird der Scan übersprungen. GuardDuty kann nicht feststellen, dass

in allen Dateiformaten ein Passwortschutz vorhanden ist. Wenn das Vorhandensein eines Kennwortschutzes nicht erkannt werden GuardDuty kann, GuardDuty wird der verschlüsselte Inhalt trotzdem gescannt.

Informationen zu den Kontingenten in Bezug auf Objektgröße, maximale Archivtiefe und weitere Informationen finden Sie unterKontingente im Malware-Schutz für S3.

Informationen darüber, ob eine Amazon S3 S3-Funktion unterstützt wird oder nicht, finden Sie unterUnterstützbarkeit der Amazon S3 S3-Funktionen.

- Unterstützt das Markieren von gescannten S3-Objekten — Wenn Sie diese Option aktivierenOptionales Markieren von Objekten auf der Grundlage des Scanergebnisses, GuardDuty wird nach jedem Malware-Scan ein Tag hinzugefügt, das den Scanstatus angibt. Sie können dieses Tag verwenden, um die tagbasierte Zugriffskontrolle (TBAC) für die S3-Objekte einzurichten. Sie können beispielsweise den Zugriff auf die S3-Objekte einschränken, die als bösartig gekennzeichnet sind und den Tag-Wert als haben. `THREATS_FOUND`
- EventBridge Amazon-Benachrichtigungen — GuardDuty sendet Ereignisse an Amazon EventBridge , wenn sich der Ressourcenstatus des Malware-Schutzplans ändert oder ein Malware-Scan des S3-Objekts abgeschlossen ist. Diese Ereignisse werden an den Standard-Event-Bus gesendet. Sie können diese Ereignisse verwenden EventBridge , um Regeln zu schreiben, die Aktionen ergreifen, z. B. die Überwachung, wann diese Ereignisse eintreten. Weitere Informationen finden Sie unter Überwachung von S3-Objektscans mit Amazon EventBridge.
- CloudWatch Metriken — Zeigen Sie CloudWatch Metriken an, um Alarme bei einem bestimmten Malware-Scanstatus zu aktivieren. Weitere Informationen finden Sie unter Statusmetriken für den S3-Objektscan in CloudWatch.

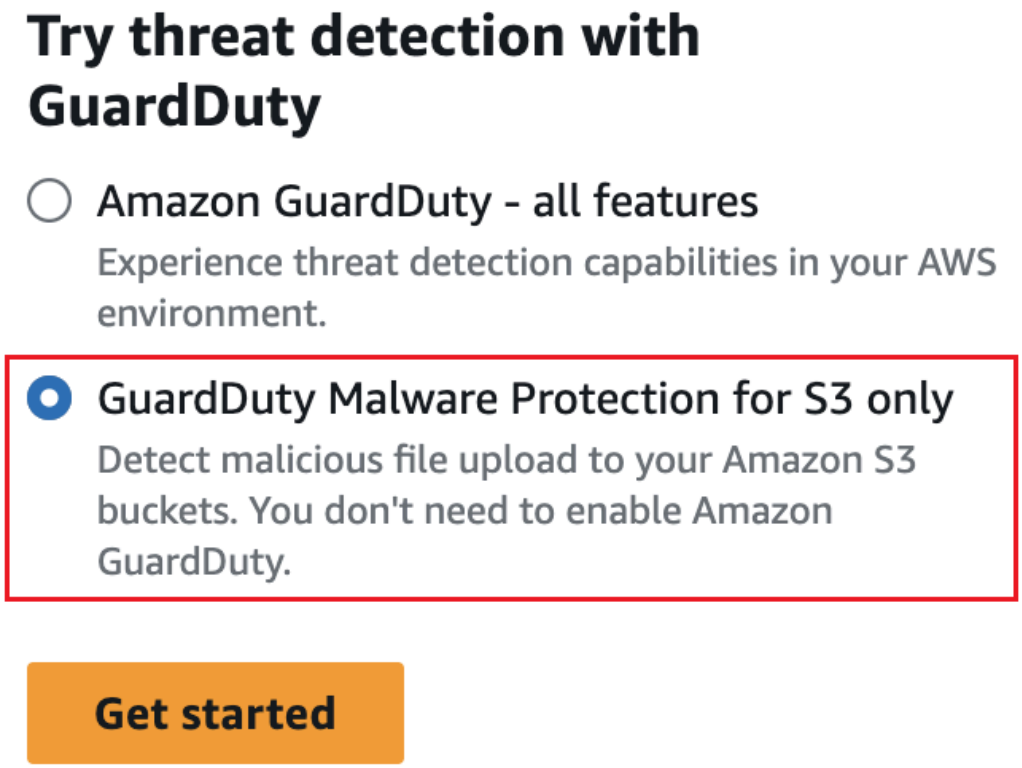
(Optional) Starten Sie eigenständig mit GuardDuty Malware Protection for S3 (nur Konsole)

Verwenden Sie diesen optionalen Schritt, wenn Sie unabhängig von Ihrem GuardDuty Status mit der Bedrohungserkennungsoption Malware Protection for S3 beginnen möchten AWS-Konto.

Wenn Sie auch andere spezielle Schutzpläne verwenden möchten GuardDuty, müssen Sie mit dem GuardDuty Amazon-Service beginnen. Informationen zu GuardDuty Schutzplänen finden Sie unterEigenschaften von GuardDuty. Wenn Sie die Aktivierung GuardDuty in Ihrem Konto bereits aktiviert haben, können Sie diesen Schritt überspringen und fortfahrenKonfiguration des Malware-Schutzes für S3 für Ihren Bucket.

Schritte für den Einstieg in die Bedrohungserkennung nur für Malware Protection for S3

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie GuardDuty Malware-Schutz nur für S3 aus. Auf diese Weise können Sie erkennen, ob eine neu hochgeladene Datei in Ihrem Amazon Simple Storage Service (Amazon S3) -Bucket möglicherweise Malware enthält.



3. Wählen Sie Erste Schritte. Sie können nun mit den Schritten unter fortfahrenKonfiguration des Malware-Schutzes für S3 für Ihren Bucket.

Konfiguration des Malware-Schutzes für S3 für Ihren Bucket

Damit Malware Protection for S3 Ihre S3-Objekte scannen und (optional) Tags zu ihnen hinzufügen kann, können Sie Servicerollen verwenden, die über die erforderlichen Berechtigungen verfügen, um in Ihrem Namen Malware-Scanaktionen durchzuführen. Weitere Informationen zur Verwendung von Servicerollen zur Aktivierung des Malware-Schutzes für S3 finden Sie unter Service Access. Diese Rolle unterscheidet sich von der serviceverknüpften Rolle von GuardDuty Malware Protection.

Wenn Sie IAM-Rollen bevorzugen, können Sie eine IAM-Rolle hinzufügen, die die erforderlichen Berechtigungen zum Scannen und (optional) Hinzufügen von Tags zu Ihren S3-Objekten enthält. GuardDuty übernimmt dann diese IAM-Rolle, um diese Aktionen in Ihrem Namen auszuführen. Sie benötigen diesen IAM-Rollennamen zum Zeitpunkt der Aktivierung dieses Schutzplans für Ihren Amazon S3-Bucket.

Wenn Sie IAM-Rollen verwenden, müssen Sie jedes Mal, wenn Sie einen Amazon S3-Bucket schützen möchten, beide in diesem Abschnitt aufgeführten Schritte ausführen.

Um den Malware-Schutz für S3 zu aktivieren, benötigen Sie Details wie den S3-Bucket-Namen, Objektpräfixe, wenn Sie den Schutz auf bestimmte Präfixe konzentrieren möchten, und den IAM-Rollennamen mit den erforderlichen Berechtigungen.

Die Schritte bleiben dieselben, unabhängig davon, ob Sie eigenständig mit Malware Protection for S3 beginnen oder es als Teil des Dienstes aktivieren. GuardDuty

Topics

1. IAM-Rollenrichtlinie erstellen oder aktualisieren
2. Malware-Schutz für S3 für Ihren Bucket aktivieren
3. Behebung eines Fehlers mit IAM-Rollenberechtigungen

Malware-Schutz für S3 für Ihren Bucket aktivieren

Dieser Abschnitt enthält detaillierte Schritte zur Aktivierung von Malware Protection for S3 für einen Bucket in Ihrem eigenen Konto. Bevor Sie fortfahren, sollten Sie die folgenden Überlegungen überprüfen:

- Wenn Sie diesen Schutzplan über die GuardDuty Konsole aktivieren, umfasst er den Schritt zum Erstellen einer neuen Rolle oder zum Verwenden einer vorhandenen Rolle im Abschnitt Servicezugriff.
- Wenn Sie diesen Schutzplan mithilfe der GuardDuty API oder CLI aktivieren, müssen Sie dies tun, IAM-Rollenrichtlinie erstellen oder aktualisieren bevor Sie fortfahren.
- Unabhängig davon, wie Sie diesen Schutzplan aktivieren, müssen Sie über das erforderliche verfügenBerechtigungen zum Erstellen einer Ressource für den Malware-Schutzplan.

Erwägen Sie die Drosselung des Amazon S3-Buckets

Die S3-Drosselung kann die Geschwindigkeit einschränken, mit der Daten zu oder von Ihren Amazon S3-Buckets übertragen werden können. Dadurch können Malware-Scans Ihrer neu hochgeladenen Objekte möglicherweise verzögert werden.

Wenn Sie ein hohes Volumen an S3-Buckets `GET` und `PUT` Anfragen an Ihre S3-Buckets erwarten, sollten Sie erwägen, Maßnahmen zur Verhinderung von Drosselungen zu ergreifen. Informationen dazu finden Sie unter Verhindern der Amazon S3-Drosselung im Amazon Athena-Benutzerhandbuch.

Berechtigungen zum Erstellen einer Ressource für den Malware-Schutzplan

Wenn Sie Malware Protection for S3 für einen Amazon S3-Bucket aktivieren, GuardDuty wird eine Ressource für den Malware-Schutzplan erstellt, die als Kennung für den Schutzplan des Buckets dient. Wenn Sie den noch nicht verwendenAWS verwaltete Richtlinie: AmazonGuardDutyFullAccess_v2 (empfohlen), müssen Sie die folgenden Berechtigungen hinzufügen, um diese Ressource zu erstellen:

- `guardDuty:CreateMalwareProtectionPlan`
- `iam:PassRole`

Sie können das folgende Beispiel für eine benutzerdefinierte Richtlinie verwenden und das *`placeholder values`* durch die für Ihr Konto geeigneten Werte ersetzen:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::111122223333:role/role-name",
            "Condition": {
                "StringEquals": {
```

```
                    "iam:PassedToService": "malware-protection-
plan.guardduty.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:CreateMalwareProtectionPlan"
            ],
            "Resource": "*"
        }
    ]
}
```

Aktivierung des Malware-Schutzes für S3 mithilfe der GuardDuty Konsole

In den folgenden Abschnitten finden Sie eine schrittweise Anleitung, wie Sie sie in der GuardDuty Konsole erleben werden.

So aktivieren Sie Malware Protection for S3 mithilfe der Konsole GuardDuty

Geben Sie die S3-Bucket-Details ein

Gehen Sie wie folgt vor, um die Amazon S3-Bucket-Details bereitzustellen:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie den Malware-Schutz für S3 aktivieren möchten.
3. Wählen Sie im Navigationsbereich Malware Protection for S3 aus.
4. Wählen Sie im Abschnitt Geschützte Buckets die Option Enable aus, um Malware Protection for S3 für einen S3-Bucket zu aktivieren, der zu Ihrem eigenen AWS-Konto gehört.
5. Geben Sie unter Geben Sie die S3-Bucket-Details ein den Namen des Amazon S3-Buckets ein. Wählen Sie alternativ Browse S3, um einen S3-Bucket auszuwählen.

   Der AWS-Region Wert des S3-Buckets und der AWS-Konto Ort, an dem Sie den Malware-Schutz für S3 aktivieren, müssen identisch sein. Wenn Ihr Konto beispielsweise zur `us-east-1` Region gehört, muss es auch Ihre Amazon S3-Bucket-Region sein`us-east-1`.

6. Unter Präfix können Sie entweder Alle Objekte im S3-Bucket oder Objekte auswählen, die mit einem bestimmten Präfix beginnen.

   - Wählen Sie Alle Objekte im S3-Bucket aus, wenn Sie alle neu hochgeladenen Objekte im ausgewählten Bucket scannen möchten GuardDuty .
   - Wählen Sie Objekte aus, die mit einem bestimmten Präfix beginnen, wenn Sie die neu hochgeladenen Objekte scannen möchten, die zu einem bestimmten Präfix gehören.
     Mit dieser Option können Sie den Umfang des Malware-Scans nur auf die ausgewählten Objektpräfixe konzentrieren. Weitere Informationen zur Verwendung von Präfixen finden Sie unter Organisieren von Objekten in der Amazon S3-Konsole mithilfe von Ordnern im Amazon S3-Benutzerhandbuch.

     Wählen Sie Präfix hinzufügen und geben Sie das Präfix ein. Sie können bis zu fünf Präfixe hinzufügen.

Aktivieren Sie das Tagging für gescannte Objekte

Dies ist ein optionaler Schritt. Wenn Sie die Tagging-Option aktivieren, bevor ein Objekt in Ihren Bucket hochgeladen wird, GuardDuty wird nach Abschluss des Scans ein vordefiniertes Tag mit dem Schlüssel als `GuardDutyMalwareScanStatus` und dem Wert als Scanergebnis hinzugefügt. Um Malware Protection for S3 optimal nutzen zu können, empfehlen wir, die Option zum Hinzufügen von Tags zu den S3-Objekten nach Abschluss des Scans zu aktivieren. Es fallen die Standardkosten für das S3-Objektkennzeichnen an. Weitere Informationen finden Sie unter Preise und Nutzungskosten für Malware Protection for S3.

Warum sollten Sie das Tagging aktivieren?

- Die Aktivierung des Tagging ist eine der Möglichkeiten, sich über das Ergebnis des Malware-Scans zu informieren. Hinweise zum Ergebnis eines S3-Scans auf Schadsoftware finden Sie unterÜberwachung von S3-Objektscans in Malware Protection for S3.
- Richten Sie eine tagbasierte Zugriffskontrollrichtlinie (TBAC) für Ihren S3-Bucket ein, der das potenziell schädliche Objekt enthält. Informationen zu Überlegungen und zur Implementierung der tagbasierten Zugriffskontrolle (TBAC) finden Sie unter. Verwenden von tagbasierter Zugriffskontrolle (TBAC) mit Malware Protection for S3

Überlegungen zum Hinzufügen eines Tags GuardDuty zu Ihrem S3-Objekt:

- Standardmäßig können Sie einem Objekt bis zu 10 Tags zuordnen. Weitere Informationen finden Sie unter Kategorisieren Ihres Speichers mithilfe von Tags im Amazon S3-Benutzerhandbuch.

  Wenn alle 10 Tags bereits verwendet werden, GuardDuty kann das vordefinierte Tag dem gescannten Objekt nicht hinzugefügt werden. GuardDuty veröffentlicht das Scanergebnis auch auf Ihrem EventBridge Standard-Event-Bus. Weitere Informationen finden Sie unter Überwachung von S3-Objektscans mit Amazon EventBridge.
- Wenn die ausgewählte IAM-Rolle nicht die Berechtigung GuardDuty zum Taggen des S3-Objekts enthält, können Sie diesem gescannten S3-Objekt kein Tag hinzufügen, auch wenn GuardDuty das Tagging für Ihren geschützten Bucket aktiviert ist. Weitere Informationen zur erforderlichen IAM-Rollenberechtigung für das Taggen finden Sie unter. IAM-Rollenrichtlinie erstellen oder aktualisieren

  GuardDuty veröffentlicht das Scan-Ergebnis auch auf Ihrem EventBridge Standard-Event-Bus. Weitere Informationen finden Sie unter Überwachung von S3-Objektscans mit Amazon EventBridge.

Um eine Option unter „Gescannte Objekte kennzeichnen“ auszuwählen

- Wenn Sie Ihren gescannten S3-Objekten Tags hinzufügen möchten GuardDuty , wählen Sie Objekte taggen aus.
- Wenn Sie Ihren gescannten S3-Objekten keine Tags hinzufügen möchten GuardDuty , wählen Sie Objekte nicht taggen aus.

Zugriff auf Services

Gehen Sie wie folgt vor, um eine vorhandene Servicerolle auszuwählen oder eine neue Servicerolle zu erstellen, die über die erforderlichen Berechtigungen verfügt, um in Ihrem Namen Malware-Scanaktionen durchzuführen. Zu diesen Aktionen können das Scannen der neu hochgeladenen S3-Objekte und (optional) das Hinzufügen von Tags zu diesen Objekten gehören. Informationen zu den Berechtigungen, die diese Rolle haben wird, finden Sie unterIAM-Rollenrichtlinie erstellen oder aktualisieren.

Im Abschnitt Servicezugriff können Sie eine der folgenden Aktionen ausführen:

1. Eine neue Servicerolle erstellen und verwenden — Sie können eine neue Servicerolle erstellen, die über die erforderlichen Berechtigungen für die Durchführung eines Malware-Scans verfügt.

Unter dem Rollennamen können Sie wählen, ob Sie den von vorausgefüllten Namen verwenden GuardDuty oder einen aussagekräftigen Namen Ihrer Wahl eingeben möchten, um die Rolle zu identifizieren. Zum Beispiel `GuardDutyS3MalwareScanRole`. Der Rollenname muss aus 1 bis 64 Zeichen bestehen. Gültige Zeichen sind a-z, A-Z 0-9 und '+=, .@-_'.

2. Eine vorhandene Servicerolle verwenden — Sie können eine vorhandene Servicerolle aus der Liste mit den Servicerollennamen auswählen.

   a. Unter Richtlinienvorlage können Sie die Richtlinie für Ihren S3-Bucket einsehen. Stellen Sie sicher, dass Sie im Abschnitt „S3-Bucket-Details eingeben“ einen S3-Bucket eingegeben oder ausgewählt haben.

   b. Wählen Sie unter Servicerollenname eine Servicerolle aus der Liste der Servicerollen aus.

Sie können die Richtlinie entsprechend Ihren Anforderungen ändern. Weitere Informationen dazu, wie Sie eine IAM-Rolle erstellen oder aktualisieren können, finden Sie unter IAM-Rollenrichtlinie erstellen oder aktualisieren.

Informationen zu Problemen mit IAM-Rollenberechtigungen finden Sie unter. Behebung eines Fehlers mit IAM-Rollenberechtigungen

(Optional) Kennzeichnen Sie die Paket-ID für den Malware-Schutz

Dies ist ein optionaler Schritt, der Ihnen hilft, der Ressource des Malware Protection-Plans Tags hinzuzufügen, die für Ihre S3-Bucket-Ressource erstellt würden.

Jedes Tag besteht aus zwei Teilen: einem Tag-Schlüssel und einem optionalen Tag-Wert. Weitere Informationen zum Taggen und seinen Vorteilen finden Sie unter Ressourcen zum Taggen AWS .

So fügen Sie Tags zu Ihrer Ressource für den Malware Protection-Plan hinzu

1. Geben Sie den Schlüssel und einen optionalen Wert für das Tag ein. Sowohl der Tag-Schlüssel als auch der Tag-Wert unterscheiden zwischen Groß- und Kleinschreibung. Informationen zu den Namen des Tag-Schlüssels und des Tag-Werts finden Sie unter Beschränkungen und Anforderungen für Tag-Benennungen.
2. Um der Ressource Ihres Malware Protection-Plans weitere Tags hinzuzufügen, wählen Sie Neues Tag hinzufügen und wiederholen Sie den vorherigen Schritt. Sie können bis zu 50 Tags für jede -Ressource hinzufügen.
3. Wählen Sie Enable (Aktivieren) aus.

Aktivieren Sie den Malware-Schutz für S3 mit API/CLI

Dieser Abschnitt enthält die Schritte, mit denen Sie den Malware-Schutz für S3 programmgesteuert in Ihrer AWS Umgebung aktivieren möchten. Dazu ist die IAM-Rolle Amazon Resource Name (ARN) erforderlich, die Sie in diesem Schritt erstellt haben -. IAM-Rollenrichtlinie erstellen oder aktualisieren

Um Malware Protection for S3 programmgesteuert zu aktivieren, verwenden Sie API/CLI

- Durch die Verwendung der API

  Führen Sie den aus CreateMalwareProtectionPlan, um Malware Protection for S3 für einen Bucket zu aktivieren, der zu Ihrem eigenen Konto gehört.

- Indem Sie AWS CLI

  Je nachdem, wie Sie Malware Protection for S3 aktivieren möchten, enthält die folgende Liste AWS CLI Beispielbefehle für einen bestimmten Anwendungsfall. Wenn Sie diese Befehle ausführen, ersetzen Sie das *placeholder examples shown in red* durch die Werte, die für Ihr Konto geeignet sind.

  AWS CLI Beispielbefehle

  - Verwenden Sie den folgenden AWS CLI Befehl, um Malware Protection for S3 für einen Bucket ohne Tagging für gescannte S3-Objekte zu aktivieren:

    ```
    aws guardduty create-malware-protection-plan --role
     "arn:aws:iam::111122223333:role/role-name" --protected-resource
     "S3Bucket"={"BucketName"="amzn-s3-demo-bucket1"}
    ```

  - Verwenden Sie den folgenden AWS CLI Befehl, um Malware Protection for S3 für einen Bucket mit bestimmten Objektpräfixen und ohne Tagging für gescannte S3-Objekte zu aktivieren:

    ```
    aws guardduty create-malware-protection-plan --role
     "arn:aws:iam::111122223333:role/role-name" --protected-resource '{"S3Bucket":
    {"BucketName":"amzn-s3-demo-bucket1", "ObjectPrefixes": ["Object1","Object1"]}}'
    ```

  - Verwenden Sie den folgenden AWS CLI Befehl, um Malware Protection for S3 für einen Bucket zu aktivieren, in dem das Tagging von gescannten S3-Objekten aktiviert ist:

    ```
    aws guardduty create-malware-protection-plan --role
     "arn:aws:iam::111122223333:role/role-name" --protected-resource
    ```

```
"S3Bucket"={"BucketName"="amzn-s3-demo-bucket1"} --actions
"Tagging"={"Status"="ENABLED"}
```

Nachdem Sie diese Befehle erfolgreich ausgeführt haben, wird eine eindeutige Malware Protection-Plan-ID generiert. Um Aktionen wie das Aktualisieren oder Deaktivieren des Schutzplans für Ihren Bucket durchzuführen, benötigen Sie diese Malware Protection-Plan-ID.

Informationen zu Problemen mit IAM-Rollenberechtigungen finden Sie unter. Behebung eines Fehlers mit IAM-Rollenberechtigungen

IAM-Rollenrichtlinie erstellen oder aktualisieren

Damit Malware Protection for S3 Ihre S3-Objekte scannen und (optional) Tags zu ihnen hinzufügen kann, können Sie Servicerollen verwenden, die über die erforderlichen Berechtigungen verfügen, um in Ihrem Namen Malware-Scanaktionen durchzuführen. Weitere Informationen zur Verwendung von Servicerollen zur Aktivierung des Malware-Schutzes für S3 finden Sie unter Service Access. Diese Rolle unterscheidet sich von der serviceverknüpften Rolle von GuardDuty Malware Protection.

Wenn Sie IAM-Rollen bevorzugen, können Sie eine IAM-Rolle hinzufügen, die die erforderlichen Berechtigungen zum Scannen und (optional) Hinzufügen von Tags zu Ihren S3-Objekten enthält. Sie müssen eine IAM-Rolle erstellen oder eine vorhandene Rolle aktualisieren, um diese Berechtigungen einzubeziehen. Da diese Berechtigungen für jeden Amazon S3-Bucket erforderlich sind, für den Sie den Malware-Schutz für S3 aktivieren, müssen Sie diesen Schritt für jeden Amazon S3-Bucket ausführen, den Sie schützen möchten.

In der folgenden Liste wird erläutert, wie bestimmte Berechtigungen dazu beitragen, den Malware-Scan in Ihrem Namen GuardDuty durchzuführen:

- Erlauben Sie Amazon EventBridge Actions, die EventBridge verwaltete Regel zu erstellen und zu verwalten, sodass Malware Protection for S3 Ihre S3-Objektbenachrichtigungen abhören kann.

  Weitere Informationen finden Sie unter Von Amazon EventBridge verwaltete Regeln im EventBridge Amazon-Benutzerhandbuch.
- Erlauben Sie Amazon S3 und EventBridge Aktionen, Benachrichtigungen EventBridge für alle Ereignisse in diesem Bucket zu senden

  Weitere Informationen finden Sie unter Enabling Amazon EventBridge im Amazon S3-Benutzerhandbuch.

- Erlauben Sie Amazon S3-Aktionen den Zugriff auf das hochgeladene S3-Objekt und fügen Sie dem gescannten S3-Objekt ein vordefiniertes Tag hinzu. `GuardDutyMalwareScanStatus` Wenn Sie ein Objektpräfix verwenden, fügen Sie eine `s3:prefix` Bedingung nur für die Zielpräfixe hinzu. Dies GuardDuty verhindert den Zugriff auf alle S3-Objekte in Ihrem Bucket.
- Erlauben Sie KMS-Schlüsselaktionen den Zugriff auf das Objekt, bevor Sie ein Testobjekt scannen und in Buckets mit der unterstützten DSSE-KMS SSE-KMS UND-Verschlüsselung platzieren.

> **Note**
>
> Dieser Schritt ist jedes Mal erforderlich, wenn Sie Malware Protection for S3 für einen Bucket in Ihrem Konto aktivieren. Wenn Sie bereits über eine IAM-Rolle verfügen, können Sie deren Richtlinie aktualisieren, sodass sie die Details einer anderen Amazon S3-Bucket-Ressource enthält. Das Hinzufügen von IAM-Richtlinienberechtigungen Thema enthält ein Beispiel dafür.

Verwenden Sie die folgenden Richtlinien, um eine IAM-Rolle zu erstellen oder zu aktualisieren.

Richtlinien

- Hinzufügen von IAM-Richtlinienberechtigungen
- Richtlinie für Vertrauensbeziehungen hinzufügen

Hinzufügen von IAM-Richtlinienberechtigungen

Sie können wählen, ob Sie die Inline-Richtlinie einer vorhandenen IAM-Rolle aktualisieren oder eine neue IAM-Rolle erstellen möchten. Informationen zu den Schritten finden Sie unter Erstellen einer IAM-Rolle oder Ändern einer Rollenberechtigungsrichtlinie im IAM-Benutzerhandbuch.

Fügen Sie Ihrer bevorzugten IAM-Rolle die folgende Vorlage für Berechtigungen hinzu. Ersetzen Sie die folgenden Platzhalterwerte durch entsprechende Werte, die Ihrem Konto zugeordnet sind:

- Ersetzen Sie *amzn-s3-demo-bucket* das durch Ihren Amazon S3-Bucket-Namen.

  Um dieselbe IAM-Rolle für mehr als eine S3-Bucket-Ressource zu verwenden, aktualisieren Sie eine vorhandene Richtlinie, wie im folgenden Beispiel dargestellt:

```
...
...
```

```
                "Resource": [
                    "arn:aws:s3:::amzn-s3-demo-bucket/*",
                    "arn:aws:s3:::amzn-s3-demo-bucket2/*"
                ],
                ...
                ...
```

Stellen Sie sicher, dass Sie ein Komma (,) hinzufügen, bevor Sie einen neuen ARN hinzufügen, der dem S3-Bucket zugeordnet ist. Tun Sie dies überall dort, wo Sie `Resource` in der Richtlinienvorlage auf einen S3-Bucket verweisen.

- Ersetzen *111122223333* Sie das durch Ihre AWS-Konto ID.
- Denn*us-east-1*, ersetze durch deine AWS-Region.
- Oder *APKAEIBAERJR2EXAMPLE* ersetzen Sie es durch Ihre vom Kunden verwaltete Schlüssel-ID. Wenn Ihr S3-Bucket mithilfe eines AWS KMS Schlüssels verschlüsselt ist, fügen wir die entsprechenden Berechtigungen hinzu, wenn Sie bei der Konfiguration des Malware-Schutzes für Ihren Bucket die Option Neue Rolle erstellen wählen.

```
"Resource": "arn:aws:kms:us-east-1:111122223333:key/*"
```

Vorlage für eine IAM-Rollenrichtlinie

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Sid": "AllowManagedRuleToSendS3EventsToGuardDuty",
            "Effect": "Allow",
            "Action": [
                "events:PutRule",
                "events:DeleteRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": [
                "arn:aws:events:us-east-1:111122223333:rule/DO-NOT-DELETE-
AmazonGuardDutyMalwareProtectionS3*"
            ],
            "Condition": {
```

```
                "StringLike": {
                    "events:ManagedBy": "malware-protection-
plan.guardduty.amazonaws.com"
                }
            }
        },
        {
            "Sid": "AllowGuardDutyToMonitorEventBridgeManagedRule",
            "Effect": "Allow",
            "Action": [
                "events:DescribeRule",
                "events:ListTargetsByRule"
            ],
            "Resource": [
                "arn:aws:events:us-east-1:111122223333:rule/DO-NOT-DELETE-
AmazonGuardDutyMalwareProtectionS3*"
            ]
        },
        {
            "Sid": "AllowPostScanTag",
            "Effect": "Allow",
            "Action": [
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:PutObjectVersionTagging",
                "s3:GetObjectVersionTagging"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        },
        {
            "Sid": "AllowEnableS3EventBridgeEvents",
            "Effect": "Allow",
            "Action": [
                "s3:PutBucketNotification",
                "s3:GetBucketNotification"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket"
            ]
        },
        {
            "Sid": "AllowPutValidationObject",
```

```
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/malware-protection-resource-
validation-object"
            ]
        },
        {
            "Sid": "AllowCheckBucketOwnership",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket"
            ]
        },
        {
           "Sid": "AllowMalwareScan",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        },
        {
            "Sid": "AllowDecryptForMalwareScan",
            "Effect": "Allow",
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:us-
east-1:111122223333:key/APKAEIBAERJR2EXAMPLE",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": "s3.us-east-1.amazonaws.com"
                }
            }
```

```
        }
    ]
}
```

Richtlinie für Vertrauensbeziehungen hinzufügen

Fügen Sie Ihrer IAM-Rolle die folgende Vertrauensrichtlinie hinzu. Informationen zu den Schritten finden Sie unter Ändern einer Rollenvertrauensrichtlinie.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection-plan.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Behebung eines Fehlers mit IAM-Rollenberechtigungen

GuardDuty Prüft bei der Aktivierung von Malware Protection for S3, ob Ihre IAM-Servicerolle über die erforderlichen Berechtigungen verfügt, um den Besitz eines Amazon S3 S3-Buckets zu überprüfen. Wenn diese Berechtigungen fehlen oder falsch konfiguriert sind, wird möglicherweise die folgende Meldung angezeigt:

```
"message": "The request was rejected because provided IAM role does not have the
 required permissions to validate S3 bucket ownership."
"type": "InvalidInputException"
```

Die folgenden Szenarien können Ihnen bei der Behebung dieses Fehlers helfen:

Fehlende IAM-Rollenberechtigungen

- Die IAM-Rolle muss über die erforderlichen Berechtigungen verfügen, damit Malware Protection for S3 diese Rolle übernehmen kann.
- GuardDuty bestätigt den Besitz des Buckets mit der `"s3:ListBucket"` entsprechenden Genehmigung. Dies muss in der IAM-Rolle, die Sie verwenden, vorhanden sein.

Informationen zu den Berechtigungen finden Sie unterIAM-Rollenrichtlinie erstellen oder aktualisieren.

Verfügbarkeit von IAM-Rollen

- Wenn Sie eine neue IAM-Rolle erstellen, warten Sie einige Minuten, bis die Änderungen endgültig konsistent sind, bevor Sie Malware Protection for S3 aktivieren. Wenn Sie versuchen, den Schutzplan unmittelbar nach der Erstellung der Rolle zu aktivieren, schlägt die Überprüfung möglicherweise fehl.
- Für Infrastructure as Code (IaC) -Bereitstellungen GuardDuty empfiehlt es sich, eine Ressourcenabhängigkeit zu deklarieren, um sicherzustellen, dass die IAM-Rolle letztendlich konsistent ist.

  Beispielvorlagen für diese Vorgehensweise finden Sie im Repository. GuardDuty GitHub

Cross-region Aktivierung

Stellen Sie sicher, dass sich Ihr Amazon S3 S3-Bucket in derselben Region befindet, in der Sie Malware Protection for S3 aktivieren GuardDuty.

Schritte nach der Aktivierung von Malware Protection for S3

In diesem Abschnitt werden die Schritte aufgeführt, die Sie ergreifen können, nachdem Sie Malware Protection for S3 für einen Bucket aktiviert haben. Die folgenden Schritte sind in einer Reihenfolge aufgeführt, die Ihnen die Navigation durch die nächsten Schritte erleichtert:

Gehen Sie wie folgt vor, nachdem Sie Malware Protection for S3 für Ihren Bucket aktiviert haben

1. Ressourcenrichtlinie für tagbasierte Zugriffskontrolle (TBAC) hinzufügen — Wenn Sie Tagging aktivieren und ein Objekt in den ausgewählten Bucket hochgeladen wird, stellen Sie sicher, dass Sie die TBAC-Richtlinie zu Ihrer S3-Bucket-Ressource hinzufügen. Weitere Informationen finden Sie unter TBAC zur S3-Bucket-Ressource hinzufügen.

2. Status des Malware-Schutzplans überwachen — Überwachen Sie die Statusspalte für jeden geschützten Bucket. Informationen zu möglichen Status und deren Bedeutung finden Sie unterStatus eines geschützten Buckets anzeigen und verstehen.
3. Starten Sie einen Scan, indem Sie eine der folgenden Optionen wählen:
   - Laden Sie ein Objekt hoch:
     1. Öffnen Sie die Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/.
     2. Laden Sie eine Datei in den S3-Bucket oder das Objektpräfix hoch, für das Sie diese Funktion aktiviert haben. Die Schritte zum Hochladen einer Datei finden Sie unter Hochladen eines Objekts in Ihren Bucket im Amazon S3 S3-Benutzerhandbuch.
   - Initiieren Sie einen On-Demand-Scan: On-demand S3-Malware-Scan GuardDuty
4. S3-Objektscanstatus und Scanergebnis überwachen — Dieser Schritt beinhaltet Informationen darüber, wie Sie den Malware-Scanstatus des S3-Objekts überprüfen können.

GuardDuty Sowohl als auch der Malware-Schutz für S3 aktiviert	Malware-Schutz nur für S3 aktiviert
• Wenn diese Option aktiviert GuardDuty ist, kann sie generiert werden, Suchtyp „Malware-Schutz für S3“ um auf das Vorhandensein von Malware im gescannten S3-Objekt hinzuweisen. • Möglicherweise können Sie das Ergebnis des S3-Objektscans überprüfen, indem Sie eine oder mehrere Optionen unter verwendenÜberwachung von S3-Objektscans in Malware Protection for S3. Dazu gehören die Nutzung von Amazon EventBridge, CloudWatch Metriken für den Malware-Schutzplan und das Markieren gescannter Objekte.	Möglicherweise können Sie das Ergebnis des S3-Objektscans überprüfen, indem Sie eine oder mehrere Optionen unter Überwachung von S3-Objektscans in Malware Protection for S3 verwenden. Dazu gehören die Nutzung von Amazon EventBridge, CloudWatch Metriken für den Malware-Schutzplan und das Markieren gescannter Objekte.

On-demand S3-Malware-Scan GuardDuty

GuardDuty Malware Protection for S3 überwacht kontinuierlich neue S3-Uploads. Für Objekte, die vor der Aktivierung des Schutzes vorhanden waren, oder um zuvor gescannte Objekte erneut zu scannen, können Sie einen S3-Malware-Scan auf Anfrage starten, sobald Sie den GuardDuty Malware-Schutzplan für Ihren Bucket aktiviert haben.

On-demand Beim Malware-Scan wird die IAM-Rolle des Malware Protection Plans für den Objektzugriff und die Konfiguration verwendet. Der Scan überschreibt jedes Präfix, das im Malware-Schutzplan für den Bucket konfiguriert wurde.

> **Note**
>
> Das Malware Protection for S3-Kontingent gilt für Malware-Scans auf Abruf. Weitere Informationen finden Sie unterKontingente im Malware-Schutz für S3.
> Weitere Informationen zu Preisen erhalten Sie unter Preise und Nutzungskosten für Malware Protection for S3.

Voraussetzungen

Bevor Sie einen Malware-Scan auf Abruf starten können, muss Ihr Konto die folgenden Voraussetzungen erfüllen:

- Der Malware-Schutz für S3 ist im Ziel-Bucket aktiviert. Weitere Informationen finden Sie unter Konfiguration des Malware-Schutzes für S3 für Ihren Bucket.
- Die AWS verwaltete Richtlinie: AmazonGuardDutyFullAccess_v2 (empfohlen) Richtlinie ist dem IAM-Benutzer oder der IAM-Rolle zugeordnet, die die API aufruft.

Starten Sie den Malware-Scan auf Abruf

Verwenden Sie den SendObjectMalwareScanAPI-Vorgang, für den der S3-Objektpfad als Eingabe erforderlich ist.

API/CLI

Sie können entweder die neueste Version des Objekts scannen oder eine bestimmte Version für den Scan angeben.

Um eine bestimmte Version eines Objekts zu scannen:

```
aws guardduty send-object-malware-scan --s3-object '{"Bucket":
 "amzn-s3-demo-bucket", "Key": "APKAEIBAERJR2EXAMPLE", "VersionId":
 "d41d8cd98f00b204e9800998eEXAMPLE"}'
```

Um die neueste Version eines Objekts zu scannen:

```
aws guardduty send-object-malware-scan --s3-object '{"Bucket": "amzn-s3-demo-
bucket", "Key": "APKAEIBAERJR2EXAMPLE"}'
```

> **Important**
>
> Ein erfolgreicher API-Aufruf bestätigt, dass die Scananforderung akzeptiert wurde. Es ist jedoch wichtig, die Scanergebnisse zu überwachen, um einen erfolgreichen Abschluss sicherzustellen und Probleme zu identifizieren, z. B. Fehler beim Zugriff auf das Objekt. Weitere Informationen finden Sie unter Überwachung von S3-Objektscans in Malware Protection for S3.

Verwenden von tagbasierter Zugriffskontrolle (TBAC) mit Malware Protection for S3

Wenn Sie Malware Protection for S3 für Ihren Bucket aktivieren, können Sie optional das Tagging aktivieren. Nach dem Versuch, ein neu hochgeladenes S3-Objekt im ausgewählten Bucket zu scannen, wird dem gescannten Objekt ein Tag GuardDuty hinzugefügt, um den Status des Malware-Scans anzugeben. Wenn Sie das Tagging aktivieren, fallen direkte Nutzungskosten an. Weitere Informationen finden Sie unter Preise und Nutzungskosten für Malware Protection for S3.

GuardDuty verwendet ein vordefiniertes Tag mit dem Schlüssel als `GuardDutyMalwareScanStatus` und dem Wert als einem der Malware-Scan-Status. Hinweise zu diesen Werten finden Sie unterthe section called “Status des potenziellen Scans und Status der Ergebnisse des S3-Objekts”.

Überlegungen GuardDuty zum Hinzufügen eines Tags zu Ihrem S3-Objekt:

- Standardmäßig können Sie einem Objekt bis zu 10 Tags zuordnen. Weitere Informationen finden Sie unter Kategorisieren Ihres Speichers mithilfe von Tags im Amazon S3 S3-Benutzerhandbuch.

Wenn alle 10 Tags bereits verwendet werden, GuardDuty kann das vordefinierte Tag dem gescannten Objekt nicht hinzugefügt werden. GuardDuty veröffentlicht das Scanergebnis auch in Ihrem EventBridge Standard-Event-Bus. Weitere Informationen finden Sie unter Überwachung von S3-Objektscans mit Amazon EventBridge.

- Wenn die gewählte IAM-Rolle nicht über die Berechtigung GuardDuty zum Taggen des S3-Objekts verfügt, können Sie diesem gescannten S3-Objekt auch dann kein Tag hinzufügen, GuardDuty wenn das Tagging für Ihren geschützten Bucket aktiviert ist. Weitere Informationen zu den erforderlichen IAM-Rollenberechtigungen für das Tagging finden Sie unter. IAM-Rollenrichtlinie erstellen oder aktualisieren

  GuardDuty veröffentlicht das Scanergebnis auch in Ihrem EventBridge Standard-Event-Bus. Weitere Informationen finden Sie unter Überwachung von S3-Objektscans mit Amazon EventBridge.

TBAC zur S3-Bucket-Ressource hinzufügen

Sie können die S3-Bucket-Ressourcenrichtlinien verwenden, um die tagbasierte Zugriffskontrolle (TBAC) für Ihre S3-Objekte zu verwalten. Sie können bestimmten Benutzern Zugriff gewähren, damit sie auf das S3-Objekt zugreifen und es lesen können. Wenn Sie über eine Organisation verfügen, die mithilfe von erstellt wurde AWS Organizations, müssen Sie sicherstellen, dass niemand die von hinzugefügten Tags ändern kann GuardDuty. Weitere Informationen finden Sie im Benutzerhandbuch unter Verhindern, dass Tags nur von autorisierten AWS Organizations Benutzern geändert werden. Das Beispiel, das im verlinkten Thema verwendet wird, erwähnt`ec2`. Wenn Sie dieses Beispiel verwenden, ersetzen Sie es *`ec2`* durch`s3`.

In der folgenden Liste wird erklärt, was Sie mit TBAC tun können:

- Verhindern Sie, dass alle Benutzer außer dem Service Principal von Malware Protection for S3 die S3-Objekte lesen, die noch nicht mit dem folgenden Tag-Schlüssel-Wert-Paar gekennzeichnet sind:

  `GuardDutyMalwareScanStatus:`*`Potential key value`*

- Erlaubt nur GuardDuty das Hinzufügen des Tag-Schlüssels `GuardDutyMalwareScanStatus` mit Wert als Scanergebnis zu einem gescannten S3-Objekt. Mit der folgenden Richtlinienvorlage können bestimmte Benutzer, die Zugriff haben, das Schlüssel-Wert-Paar des Tags möglicherweise außer Kraft setzen.

Beispiel für eine S3-Bucket-Ressourcenrichtlinie:

Ersetzen Sie die folgenden Platzhalterwerte in der Beispielrichtlinie:

- *IAM-role-name*- Geben Sie die IAM-Rolle, die Sie für die Konfiguration von Malware Protection for S3 verwendet haben, in Ihrem Bucket an.
- *555555555555*— Geben Sie den Bucket an, der dem geschützten Bucket AWS-Konto zugeordnet ist.
- *amzn-s3-demo-bucket*- Geben Sie den Namen des geschützten Buckets an.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Sid": "NoReadUnlessClean",
            "Effect": "Deny",
            "NotPrincipal": {
                "AWS": [
                "arn:aws:sts::555555555555:assumed-role/IAM-role-name/
GuardDutyMalwareProtection",
                "arn:aws:iam::555555555555:role/IAM-role-name"
                ]
            },
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:ExistingObjectTag/GuardDutyMalwareScanStatus":
 "NO_THREATS_FOUND"
                }
            }
        },
        {
            "Sid": "OnlyGuardDutyCanTagScanStatus",
            "Effect": "Deny",
            "NotPrincipal": {
                "AWS": [
```

```
                    "arn:aws:sts::555555555555:assumed-role/IAM-role-name/
GuardDutyMalwareProtection",
                    "arn:aws:iam::555555555555:role/IAM-role-name"
                ]
            },
            "Action": "s3:PutObjectTagging",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "s3:RequestObjectTagKeys": "GuardDutyMalwareScanStatus"
                }
            }
        }
    ]
}
```

Weitere Informationen zum Taggen Ihrer S3-Ressource finden Sie unter Tagging- und Zugriffskontrollrichtlinien.

Status eines geschützten Buckets anzeigen und verstehen

Nach der Aktivierung von Malware Protection for S3 für einen Bucket gibt der Status an, ob die Funktion wie erwartet konfiguriert ist und funktioniert. Dieser Status ist mit einer eindeutigen ID (Malware Protection Plan Identifier) verknüpft. GuardDuty erstellt diese ID zum Zeitpunkt der Aktivierung der Funktion.

Gehen Sie wie folgt vor, um den Status Ihres geschützten Buckets einzusehen:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich die Option Malware Protection for S3 aus.
3. Sehen Sie sich in der Tabelle Geschützte Buckets die entsprechende Statusspalte für Ihren S3-Bucket an.

In der folgenden Tabelle werden die Statuswerte aufgeführt und beschrieben, die mit der Ressource Ihres Malware-Schutzplans verknüpft sind. Wenn Sie wissen, was diese Status für Ihren geschützten Bucket bedeuten, können Sie besser sicherstellen, dass dieser einen automatischen Malware-Scan GuardDuty einleitet, wenn ein Objekt hochgeladen wird.

Status	Description
Aktiv	Ihr S3-Bucket wurde erfolgreich mit Malware Protection for S3 konfiguriert. Wenn der Status Aktiv lautet, wird der Status durch Änderunge n an der IAM-Rolle (Löschen oder Ändern von Berechtigungen) nicht auf Warnung oder Fehler aktualisiert. Wir empfehlen, den Scanstatus kontinuierlich mit einer der unter beschriebenen Methoden zu überwachen. Überwachung von S3-Objektscans
Warnung * -	Der Malware-Schutz für S3 ist so konzipiert, dass er nicht beeinträchtigt wird, wenn eine Warnung angezeigt wird. Wenn GuardDuty ein neues S3-Objekt entdeckt wird, wird ein Malware-Scan eingeleitet. Nach erfolgreicher Initiierung des Scans kann es einige Minuten dauern, bis der Wert in der Spalte Status auf Aktiv geändert wird. Sie erhalten eine EventBridge Benachrichtigung, nachdem der Wert der Statusspalte aktualisi ert wurde.
Fehler * -	Ihr Bucket ist nicht geschützt. Keiner der mit diesem S3-Bucket verknüpften Malware-Scans wird abgeschlossen. Es könnte eine oder mehrere mögliche Hauptursachen geben.

* Informationen zu potenziellen Problemen und den entsprechenden Schritten zu ihrer Behebung finden Sie unterFehlerbehebung beim Status des Malware-Schutzplans.

Überwachung von S3-Objektscans in Malware Protection for S3

Wenn Sie Malware Protection for S3 mit einer GuardDuty Detektor-ID verwenden und Ihr Amazon S3 S3-Objekt potenziell bösartig ist, GuardDuty wird Folgendes generiertSuchtyp „Malware-Schutz für S3“. Mithilfe der GuardDuty Konsole und der APIs können Sie sich die generierten Ergebnisse ansehen. Informationen zum Verständnis dieses Ergebnistyps finden Sie unterErkenntnisdetails.

Wenn Sie Malware Protection for S3 ohne Aktivierung verwenden GuardDuty (keine Detektor-ID), GuardDuty können auch dann keine Ergebnisse generiert werden, wenn Ihr gescanntes Amazon S3 S3-Objekt potenziell bösartig ist.

Inhalt

- Status des potenziellen Scans und Status der Ergebnisse des S3-Objekts
- Überwachung von S3-Objektscans mit Amazon EventBridge
- Überwachung von S3-Objektscans mit GuardDuty verwalteten Tags
- Statusmetriken für den S3-Objektscan in CloudWatch

Status des potenziellen Scans und Status der Ergebnisse des S3-Objekts

In diesem Abschnitt werden die möglichen Statuswerte für den S3-Objektscan und die Werte der Scanergebnisse erläutert.

Ein S3-Objektscan-Status gibt den Status des Malware-Scans an, z. B. abgeschlossen, übersprungen oder fehlgeschlagen.

Der Ergebnisstatus eines S3-Objektscans auf Schadsoftware gibt das Ergebnis des Scans auf der Grundlage des Scanstatuswerts an. Jeder Statuswert für das Ergebnis eines Malware-Scans wird einem Scanstatus zugeordnet.

Die folgende Liste enthält die potenziellen Ergebniswerte für den S3-Objektscan. Wenn Sie das Tagging aktiviert haben, können Sie das Scanergebnis anhand von Verwendung von S3-Objekt-Tags überwachen. Nach dem Scan hat der Tag-Wert einen der folgenden Scan-Ergebniswerte.

Statuswerte für die Ergebnisse der S3-Objektsuche nach potenzieller Schadsoftware

- `NO_THREATS_FOUND`— es GuardDuty wurde keine potenzielle Bedrohung im Zusammenhang mit dem gescannten Objekt festgestellt.
- `THREATS_FOUND`— hat eine potenzielle Bedrohung im Zusammenhang mit dem gescannten Objekt GuardDuty erkannt.
- `UNSUPPORTED`— Es gibt mehrere Gründe, warum Malware Protection for S3 einen Scan überspringt. Mögliche Gründe sind kennwortgeschützte Dateien, Archive mit extrem hohen Komprimierungsraten und die möglicherweise nicht Malware-Schutz für S3-Kontingente verfügbare Unterstützung für bestimmte Amazon S3 S3-Funktionen. Weitere Informationen finden Sie unter Funktionen des Malware-Schutzes für S3.
- `ACCESS_DENIED`— GuardDuty kann zum Scannen nicht auf dieses Objekt zugreifen. Überprüfen Sie die mit diesem Bucket verknüpften IAM-Rollenberechtigungen. Weitere Informationen finden Sie unter IAM-Rollenrichtlinie erstellen oder aktualisieren.

Wenn Sie das S3-Objekt-Tagging nach dem Scan aktiviert haben, finden Sie weitere Informationen unter. Behebung von Fehlern bei S3-Objekt-Tags nach dem Scannen

- `FAILED`— Dieses Objekt GuardDuty kann aufgrund eines internen Fehlers nicht nach Schadsoftware gescannt werden.

Die folgende Liste enthält mögliche Statuswerte für S3-Objektscans und deren Zuordnung zum Ergebnis des S3-Objektscans.

Werte für den Status potenzieller S3-Objektscans

- Abgeschlossen — Der Scan wurde erfolgreich abgeschlossen und gibt an, ob das S3-Objekt Schadsoftware enthält. In diesem Fall könnte der potenzielle Ergebniswert des S3-Objektscans entweder `THREATS_FOUND` oder sein`NO_THREATS_FOUND`.
- Übersprungen — GuardDuty überspringt einen Malware-Scan, wenn das Scannen dieses S3-Objekts nicht von Malware Protection for S3 unterstützt wird oder wenn GuardDuty kein Zugriff auf das hochgeladene S3-Objekt im ausgewählten Bucket besteht.

  In diesem Fall könnte der potenzielle Ergebniswert für den S3-Objektscan entweder oder `UNSUPPORTED` lauten. `ACCESS_DENIED`

  GuardDuty überspringt den Scan auch, wenn die erforderliche IAM-Rolle gelöscht wird.
- Fehlgeschlagen — Ähnlich dem Ergebniswert `FAILED` des S3-Objektscans bedeutet dieser Scanstatus, GuardDuty dass aufgrund eines internen Fehlers kein Malware-Scan für das S3-Objekt durchgeführt werden konnte.

Wenn der Scanstatus lautet`SKIPPED`, enthält die EventBridge Benachrichtigung für das Ergebnis des S3-Objektscans ein `statusReasons` Feld dar`in scanResultDetails`. Dieses Feld ist eine Liste von Zeichenketten, die den genauen Grund angeben, warum der Scan übersprungen wurde. In der folgenden Tabelle werden die möglichen `statusReasons` Werte beschrieben.

Grund für den Status	Status der Scanergebnisse	Description
`UNAUTHORIZED_TO_GET_OBJECT`	`ACCESS_DENIED`	Malware Protection for S3 ist nicht berechtigt, das S3-Objekt zu lesen, oder das S3-

Grund für den Status	Status der Scanergebnisse	Description
		Objekt ist nicht vorhanden. Stellen Sie sicher, dass die IAM-Rolle, die dem geschützten Bucket zugeordnet ist, über die erforderlichen Berechtigungen verfügt und dass alle AWS KMS Bucket-Richtlinien es der Rolle ermöglichen, Objekte zu entschlüsseln.
`UNAUTHORIZED_TO_ASSUME_ROLE`	`ACCESS_DENIED`	Malware Protection for S3 kann die für den geschützten Bucket konfigurierte IAM-Rolle nicht übernehmen. Stellen Sie sicher, dass die Vertrauensrichtlinie für Rollen es Malware Protection for S3 ermöglicht, die Rolle zu übernehmen.
`SSE_C_ENCRYPTED_OBJECT`	`ACCESS_DENIED`	Das S3-Objekt ist mit einem vom Kunden bereitgestellten Verschlüsselungsschlüssel (SSE-C) verschlüsselt. GuardDuty kann nicht auf Objekte zugreifen, die mit SSE-C verschlüsselt sind. Weitere Informationen finden Sie unter Unterstützbarkeit der Amazon S3 S3-Funktionen.
`OBJECT_E_TAG_CHANGED`	`ACCESS_DENIED`	Das S3-Objekt-ETag hat sich zwischen dem Zeitpunkt, an dem der Scan initiiert wurde, und dem GuardDuty Versuch, das Objekt zu lesen, geändert. Der nachfolgende Upload oder die neue Version wird gescannt.
`BUCKET_NOT_FOUND`	`ACCESS_DENIED`	Der mit dem Scan verknüpfte S3-Bucket ist nicht mehr vorhanden.

Grund für den Status	Status der Scanergebnisse	Description
UNSUPPORTED_STORAGE_CLASS	UNSUPPORTED	Das S3-Objekt verwendet eine Speicherklasse, die von Malware Protection for S3 nicht unterstützt wird. Weitere Informationen finden Sie unter Unterstützbarkeit der Amazon S3 S3-Funktionen.
OBJECT_SIZE_LIMIT_EXCEEDED	UNSUPPORTED	Die S3-Objektgröße überschreitet die maximale Dateigrößenbeschränkung für Malware Protection for S3. Weitere Informationen finden Sie unter Malware-Schutz für S3-Kontingente.
PASSWORD_PROTECTED	UNSUPPORTED	Das Objekt ist kennwortgeschützt.
EXTRACTED_FILE_LIMIT_EXCEEDED	UNSUPPORTED	Das Archiv enthält mehr Dateien als die zulässige Höchstmenge. Weitere Informationen finden Sie unter Malware-Schutz für S3-Kontingente.
EXTRACTED_LEVEL_LIMIT_EXCEEDED	UNSUPPORTED	Das Archiv überschreitet die maximal zulässige Verschachtelungstiefe.
EXTRACTED_BYTE_LIMIT_EXCEEDED	UNSUPPORTED	Der extrahierte Archivinhalt überschreitet die maximal zulässige Bytegröße. Weitere Informationen finden Sie unter Malware-Schutz für S3-Kontingente.
EXTRACTION_RATIO_LIMIT_EXCEEDED	UNSUPPORTED	Das Archiv hat eine extrem hohe Komprimierungsrate, die die zulässige Grenze überschreitet. Weitere Informationen finden Sie unter Malware-Schutz für S3-Kontingente.

Überwachung von S3-Objektscans mit Amazon EventBridge

Amazon EventBridge ist ein serverloser Event-Bus-Service, der es einfach macht, Ihre Anwendungen mit Daten aus einer Vielzahl von Quellen zu verbinden. EventBridge liefert einen Stream von Echtzeitdaten aus Ihren eigenen Anwendungen, Software-as-a-Service (SaaS-) Anwendungen und AWS Diensten und leitet diese Daten an Ziele wie Lambda weiter. Auf diese Weise können Sie Ereignisse überwachen, die in Services auftreten, und ereignisgesteuerte Architekturen erstellen. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.

Als Besitzerkonto eines S3-Buckets, der mit Malware Protection for S3 geschützt ist, GuardDuty veröffentlicht er in den folgenden Szenarien EventBridge Benachrichtigungen an den Standard-Event-Bus:

- Der Ressourcenstatus des Malware-Schutzplans ändert sich für jeden Ihrer geschützten Buckets. Informationen zu den verschiedenen Status finden Sie unter. Status eines geschützten Buckets anzeigen und verstehen

  Informationen zum Einrichten der Amazon EventBridge (EventBridge) -Regel für den Ressourcenstatus finden Sie unterRessourcenstatus des Malware-Schutzplans.
- Das Ergebnis des S3-Objektscans wird in Ihrem EventBridge Standard-Event-Bus veröffentlicht.

  Das `s3Throttled` Feld gibt an, ob es beim Hochladen oder Abrufen von Speicherplatz aus Amazon S3 zu Verzögerungen gekommen ist. Der Wert `true` gibt an, dass eine Verzögerung aufgetreten ist, und `false` gibt an, dass es keine Verzögerung gab.

  Wenn `s3Throttled` es sich `true` um Ihr Scanergebnis handelt, empfiehlt Amazon S3, Präfixe so einzurichten, dass Sie die Transaktionen pro Sekunde (TPS) für jedes Präfix reduzieren können. Weitere Informationen finden Sie unter Bewährte Entwurfsmuster: Optimierung der Amazon S3 S3-Leistung im Amazon S3 S3-Benutzerhandbuch.

  Informationen zum Einrichten der Amazon EventBridge (EventBridge) -Regel für die Ergebnisse des S3-Objektscans finden Sie unterErgebnis des S3-Objektscans.
- Nach dem Scannen des Tags tritt aus den folgenden Gründen ein Fehler auf:
  - In Ihrer IAM-Rolle fehlen die Berechtigungen zum Markieren des Objekts.

    Die Hinzufügen von IAM-Richtlinienberechtigungen Vorlage enthält die Berechtigung, ein Objekt GuardDuty zu taggen.

- Die in der IAM-Rolle angegebene Bucket-Ressource oder das in der IAM-Rolle angegebene Bucket-Objekt ist nicht mehr vorhanden.
- Das zugehörige S3-Objekt hat bereits das maximale Tag-Limit erreicht. Weitere Informationen zum Tag-Limit finden Sie unter Kategorisieren Ihres Speichers mithilfe von Tags im Amazon S3 S3-Benutzerhandbuch.

Informationen zur Einrichtung der Amazon EventBridge (EventBridge) -Regel für Tag-Fehlschläge nach dem Scannen finden Sie unterPost-scan Fehlerereignisse kennzeichnen.

Regeln einrichten EventBridge

Sie können in Ihrem Konto EventBridge Regeln einrichten, um entweder den Ressourcenstatus, Ereignisse nach dem Scan-Tag oder das Ergebnis des S3-Objektscans an ein anderes AWS-Service zu senden. Als delegiertes GuardDuty Administratorkonto erhalten Sie eine Benachrichtigung über den Ressourcenstatus des Malware-Schutzplans, wenn sich der Status ändert.

Es gelten die EventBridge Standardpreise. Weitere Informationen finden Sie unter EventBridge Amazon-Preise.

Alle Werte, die in angezeigt werden, *red* sind Platzhalter für das Beispiel. Diese Werte ändern sich je nach den Werten in Ihrem Konto und je nachdem, ob Malware erkannt wurde oder nicht.

Themen

- Ressourcenstatus des Malware-Schutzplans
- Ergebnis des S3-Objektscans
- Post-scan Fehlerereignisse kennzeichnen

Ressourcenstatus des Malware-Schutzplans

Sie können ein EventBridge Ereignismuster erstellen, das auf den folgenden Szenarien basiert:

Mögliche Werte vom **Typ „Detail“**

- `"GuardDuty Malware Protection Resource Status Active"`
- `"GuardDuty Malware Protection Resource Status Warning"`
- `"GuardDuty Malware Protection Resource Status Error"`

Muster des Ereignisses

```
{
      "detail-type": ["potential detail-type"],
      "source": ["aws.guardduty"]
}
```

Beispiel für ein Benachrichtigungsschema für **`GuardDuty Malware Protection Resource Status Active`**:

```
{
    "version": "0",
    "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
    "detail-type": "GuardDuty Malware Protection Resource Status Active",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2017-12-22T18:43:48Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "eventTime": "2024-02-28T01:01:01Z",
        "s3BucketDetails": {
            "bucketName": "amzn-s3-demo-bucket"
        },
        "resourceStatus": "ACTIVE"
    }
}
```

Beispiel für ein Benachrichtigungsschema für **`GuardDuty Malware Protection Resource Status Warning`**:

```
{
    "version": "0",
    "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
    "detail-type": "GuardDuty Malware Protection Resource Status warning",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2017-12-22T18:43:48Z",
    "region": "us-east-1",
```

```
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "eventTime": "2024-02-28T01:01:01Z",
        "s3BucketDetails": {
            "bucketName": "amzn-s3-demo-bucket"
        },
        "resourceStatus": "WARNING",
        "statusReasons": [
         {
            "code": "INSUFFICIENT_TEST_OBJECT_PERMISSIONS"
         }
        ]
    }
}
```

Beispiel für ein Benachrichtigungsschema für **`GuardDuty Malware Protection Resource Status Error`**:

```
{
    "version": "0",
    "id": "fc7a35b7-83bd-3c1f-ecfa-1b8de9e7f7d2",
    "detail-type": "GuardDuty Malware Protection Resource Status Error",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2017-12-22T18:43:48Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "eventTime": "2024-02-28T01:01:01Z",
        "s3BucketDetails": {
            "bucketName": "amzn-s3-demo-bucket"
        },
        "resourceStatus": "ERROR",
        "statusReasons": [
        {
            "code": "EVENTBRIDGE_MANAGED_EVENTS_DELIVERY_DISABLED"
        }
       ]
    }
```

```
}
```

Basierend auf dem Grund dafür `resourceStatus` ERROR wird der `statusReasons` Wert aufgefüllt.

Informationen zu den Schritten zur Problembehandlung bei den folgenden Warnungen und Fehlern finden Sie unterFehlerbehebung beim Status des Malware-Schutzplans.

Ergebnis des S3-Objektscans

```
{
  "detail-type": ["GuardDuty Malware Protection Object Scan Result"],
  "source": ["aws.guardduty"]
}
```

Wenn ja `scanStatus`SKIPPED, `scanResultDetails` enthält das ein `statusReasons` Feld, das den genauen Grund angibt, warum der Scan übersprungen wurde. Hinweise zu den möglichen Werten finden Sie unterStatus des potenziellen Scans und Status der Ergebnisse des S3-Objekts.

Beispiel für ein Benachrichtigungsschema für **`NO_THREATS_FOUND`**:

```
{
    "version": "0",
    "id": "72c7d362-737a-6dce-fc78-9e27a0171419",
    "detail-type": "GuardDuty Malware Protection Object Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-02-28T01:01:01Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "COMPLETED",
        "resourceType": "S3_OBJECT",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
            "eTag": "ASIAI44QH8DHBEXAMPLE",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE",
            "s3Throttled": false
        },
        "scanResultDetails": {
```

```
            "scanResultStatus": "NO_THREATS_FOUND",
            "threats": null,
            "statusReasons": null
        }
    }
}
```

Beispiel für ein Benachrichtigungsschema für **`THREATS_FOUND`**:

```
{
    "version": "0",
    "id": "72c7d362-737a-6dce-fc78-9e27a0171419",
    "detail-type": "GuardDuty Malware Protection Object Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-02-28T01:01:01Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "COMPLETED",
        "resourceType": "S3_OBJECT",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
            "eTag": "ASIAI44QH8DHBEXAMPLE",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE",
            "s3Throttled": false
        },
        "scanResultDetails": {
            "scanResultStatus": "THREATS_FOUND",
            "threats": [
                {
                    "name": "EICAR-Test-File (not a virus)",
                    "source": "AMAZON",
                    "itemDetails": [{
                        "hash":
 "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855",
                        "itemPath": "APKAEIBAERJR2EXAMPLE"
                    }]
                }
            ],
```

```
            "statusReasons": null
        }
    }
}
```

> **Note**
>
> Das `scanResultDetails.Threats` Feld enthält nur eine Bedrohung. Standardmäßig meldet der Scan von Malware Protection for S3 die erste erkannte Bedrohung. Danach `scanStatus` ist der auf eingestelltCOMPLETED.

Beispiel für ein Benachrichtigungsschema für den Status der Scanergebnisse **UNSUPPORTED** (Übersprungen):

```
{
    "version": "0",
    "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
    "detail-type": "GuardDuty Malware Protection Object Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-02-28T01:01:01Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "SKIPPED",
        "resourceType": "S3_OBJECT",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
            "eTag": "ASIAI44QH8DHBEXAMPLE",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE",
            "s3Throttled": false
        },
        "scanResultDetails": {
            "scanResultStatus": "UNSUPPORTED",
            "threats": null,
            "statusReasons": ["PASSWORD_PROTECTED"]
        }
    }
```

```
}
```

Beispiel für ein Benachrichtigungsschema für den Status der Scanergebnisse **ACCESS_DENIED** (Übersprungen):

```
{
    "version": "0",
    "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
    "detail-type": "GuardDuty Malware Protection Object Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-02-28T01:01:01Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "SKIPPED",
        "resourceType": "S3_OBJECT",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
            "eTag": "ASIAI44QH8DHBEXAMPLE",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE",
            "s3Throttled": false
        },
        "scanResultDetails": {
            "scanResultStatus": "ACCESS_DENIED",
            "threats": null,
            "statusReasons": ["SSE_C_ENCRYPTED_OBJECT"]
        }
    }
}
```

Beispiel für ein Benachrichtigungsschema für den Status **FAILED** der Scanergebnisse:

```
{
    "version": "0",
    "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
    "detail-type": "GuardDuty Malware Protection Object Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-02-28T01:01:01Z",
```

```
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "FAILED",
        "resourceType": "S3_OBJECT",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
            "eTag": "ASIAI44QH8DHBEXAMPLE",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE",
            "s3Throttled": false
        },
        "scanResultDetails": {
            "scanResultStatus": "FAILED",
            "threats": null,
            "statusReasons": null
        }
    }
}
```

Post-scan Fehlerereignisse kennzeichnen

Muster des Ereignisses:

```
{
      "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
      "source": "aws.guardduty"
 }
```

Beispiel für ein Benachrichtigungsschema für **`ACCESS_DENIED`**:

```
{
    "version": "0",
    "id": "746acd83-d75c-5b84-91d2-dad5f13ba0d7",
    "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-06-10T16:16:08Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
```

```
    "detail": {
        "schemaVersion": "1.0",
        "eventTime": "2024-06-10T16:16:08Z",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "2024-03-10-16-16-00-7D723DE8DBE9Y2E0",
            "eTag": "0e9eeec810ad8b61d69112c15c2a5hb6",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE",
            "s3Throttled": false
        },
        "postScanActions": [{
            "actionType": "TAGGING",
            "failureReason": "ACCESS_DENIED"
        }]
    }
}
```

Beispiel für ein Benachrichtigungsschema für **`MAX_TAG_LIMIT_EXCEEDED`**:

```
{
    "version": "0",
    "id": "746acd83-d75c-5b84-91d2-dad5f13ba0d7",
    "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-06-10T16:16:08Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "eventTime": "2024-06-10T16:16:08Z",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "2024-03-10-16-16-00-7D723DE8DBE9Y2E0",
            "eTag": "0e9eeec810ad8b61d69112c15c2a5hb6",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE",
            "s3Throttled": false
        },
        "postScanActions": [{
            "actionType": "TAGGING",
            "failureReason": "MAX_TAG_LIMIT_EXCEEDED"
        }]
```

```
    }
}
```

Informationen zur Behebung dieser Fehlerursachen finden Sie unterBehebung von Fehlern bei S3-Objekt-Tags nach dem Scannen.

Überwachung von S3-Objektscans mit GuardDuty verwalteten Tags

Verwenden Sie die Option „Tagging aktivieren“, GuardDuty damit Sie Ihrem Amazon S3 S3-Objekt nach Abschluss des Malware-Scans Tags hinzufügen können.

Überlegungen zur Aktivierung von Tagging

- Wenn Sie Ihre S3-Objekte taggen, GuardDuty fallen Nutzungskosten an. Weitere Informationen finden Sie unter Preise und Nutzungskosten für Malware Protection for S3.
- Sie müssen die erforderlichen Tagging-Berechtigungen für Ihre bevorzugte IAM-Rolle behalten, die mit diesem Bucket verknüpft ist. Andernfalls GuardDuty können Sie Ihren gescannten Objekten keine Tags hinzufügen. Die IAM-Rolle umfasst bereits die Berechtigungen zum Hinzufügen von Tags zu den gescannten S3-Objekten. Weitere Informationen finden Sie unter IAM-Rollenrichtlinie erstellen oder aktualisieren.
- Standardmäßig können Sie einem S3-Objekt bis zu 10 Tags zuordnen. Weitere Informationen finden Sie unter Verwenden der tagbasierten Zugriffskontrolle (TBAC).

Nachdem Sie das Tagging für einen S3-Bucket oder bestimmte Präfixe aktiviert haben, wird jedem neu hochgeladenen Objekt, das gescannt wird, ein zugeordnetes Tag im folgenden Schlüssel-Wert-Paarformat zugewiesen:

`GuardDutyMalwareScanStatus:`*`Scan-Result-Status`*

Hinweise zu möglichen Tag-Werten finden Sie unter. Status des potenziellen Scans und Status der Ergebnisse des S3-Objekts

Behebung von Fehlern bei S3-Objekten nach dem Scannen von Tags in Malware Protection for S3

Dieser Abschnitt gilt nur für Sie, wenn Sie sich Aktivieren Sie das Tagging für gescannte Objekte in Ihrem geschützten Bucket befinden.

Wenn GuardDuty versucht wird, Ihrem gescannten S3-Objekt ein Tag hinzuzufügen, kann die Aktion des Taggens zu einem Fehler führen. Die möglichen Gründe, warum dies Ihrem Bucket passieren kann, sind `ACCESS_DENIED` und`MAX_TAG_LIMIT_EXCEEDED`. In den folgenden Themen erfahren Sie mehr über die möglichen Gründe für diese Fehlerursachen nach dem Scannen von Tags und deren Behebung.

ACCESS_DENIED

Die folgende Liste enthält mögliche Gründe, die zu diesem Problem führen können:

- Der für diesen geschützten S3-Bucket verwendeten IAM-Rolle fehlt die AllowPostScanTagBerechtigung. Stellen Sie sicher, dass die zugehörige IAM-Rolle diese Bucket-Richtlinie verwendet. Weitere Informationen finden Sie unter IAM-Rollenrichtlinie erstellen oder aktualisieren.
- Die geschützte S3-Bucket-Richtlinie erlaubt es nicht GuardDuty , diesem Objekt Tags hinzuzufügen.
- Das gescannte S3-Objekt ist nicht mehr vorhanden.

MAX_TAG_LIMIT_EXCEEDED

Standardmäßig können Sie einem S3-Objekt bis zu 10 Tags zuordnen. Weitere Informationen finden Sie unter Überlegungen GuardDuty zum Hinzufügen eines Tags zu Ihrem S3-Objekt unterAktivieren Sie das Tagging für gescannte Objekte.

Statusmetriken für den S3-Objektscan in CloudWatch

Sie können die GuardDuty Nutzung CloudWatch überwachen. Dabei werden Rohdaten gesammelt und zu lesbaren Metriken verarbeitet, die nahezu in Echtzeit verfügbar sind. Diese Statistiken werden 15 Monate lang aufbewahrt, sodass Sie auf historische Informationen zugreifen und sich einen besseren Überblick über die Leistung von Malware Protection for S3 verschaffen können. Sie können auch Alarme einrichten, die auf bestimmte Grenzwerte achten und Benachrichtigungen senden oder Aktivitäten auslösen, wenn diese Grenzwerte erreicht werden. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Die CloudWatch Metriken für Malware Protection for S3 sind auf Ressourcenebene verfügbar. Sie können diese Metriken für jede geschützte Ressource separat abfragen. Die Metriken werden im `AWS/GuardDuty/MalwareProtection` Namespace gemeldet. Sie können Alarme für bestimmte Ressourcen einrichten, um den Sicherheitsstatus zu überwachen.

Statistiken zum Status von Malware-Scans

Metrik	Beschreibung
`CompletedScanCount`	Die Anzahl der S3-Objekt-Malware-Scans, die in einem bestimmten Zeitraum abgeschlossen wurden. Gültige Abmessungen: • `Malware Protection Plan Id` `Resource Name` Einheiten: Anzahl
`FailedScanCount`	Die Anzahl der S3-Objekt-Malware-Scans, die in einem bestimmten Zeitraum fehlgeschlagen sind. Gültige Abmessungen: • `Malware Protection Plan Id` `Resource Name` Einheiten: Anzahl

`SkippedScanCount`	Die Anzahl der S3-Objekt-Malware-Scans, die in einem bestimmten Zeitraum übersprungen wurden.
	
	Gültige Abmessungen:
	
	• `Malware Protection Plan Id`
	
	`Resource Name`
	
	`Skipped Reason`

	Mögliche Werte • `Unsupported` • `MissingPermissions` Einheiten: Anzahl
Kennzahlen zu den Ergebnissen von Malware-Scans	
`InfectedScanCount`	Die Anzahl der S3-Objekt-Malware-Scans, bei denen innerhalb eines bestimmten Zeitraums potenziell schädliche Objekte erkannt wurden. Gültige Abmessungen: • `Malware Protection Plan Id` `Resource Name` Einheiten: Anzahl
`CompletedScanBytes`	Die Anzahl der in einem bestimmten Zeitraum gescannten S3-Objektbytes. Gültige Abmessungen: • `Malware Protection Plan Id` `Resource Name` Einheiten: Anzahl

> **Note**
>
> Standardmäßig handelt es sich bei den Statistiken in den CloudWatch Metriken um AVG.

Die folgenden Dimensionen werden für die Messwerte Malware Protection for S3 unterstützt.

Dimension	Beschreibung
`Malware Protection Plan Id`	Die eindeutige Kennung, die der Ressource des Malware-Schutzplans zugeordnet ist, die für Ihre geschützte Ressource GuardDuty erstellt wird.
`Resource Name`	Der Name der geschützten Ressource.
`Skipped Reason`	Der Grund, warum ein S3-Objekt-Malware-Scan übersprungen wurde. Mögliche Werte • `Unsupported` • `MissingPermissions`

Informationen zum Zugriff auf und zur Abfrage dieser Messwerte finden Sie unter Verwenden von CloudWatch Amazon-Metriken im CloudWatch Amazon-Benutzerhandbuch.

Informationen zum Einrichten von Alarmen finden Sie unter Verwenden von CloudWatch Amazon-Alarmen im CloudWatch Amazon-Benutzerhandbuch.

Fehlerbehebung

Inhalt

- Fehlerbehebung beim Status des Malware-Schutzplans
- Problembehebung bei Malware-Scan auf Abruf

Fehlerbehebung beim Status des Malware-Schutzplans

GuardDuty Zeigt für jeden geschützten Bucket den Status auf der Grundlage der Rangfolge an. Wenn ein geschützter Bucket beispielsweise Probleme sowohl in der Kategorie Fehler als auch in der Kategorie Warnung aufweist, GuardDuty wird zuerst das Problem angezeigt, das dem Fehlerstatus zugeordnet ist.

Die folgende Liste enthält die Fehler und die Warnung für den Status des Malware-Schutzplans.

Fehler

- EventBridge Die Benachrichtigung ist für diesen S3-Bucket deaktiviert
- EventBridge Eine verwaltete Regel zum Empfangen von S3-Bucket-Ereignissen fehlt
- Der S3-Bucket ist nicht mehr vorhanden

Warnung

Das Testobjekt konnte nicht platziert werden

EventBridge Die Benachrichtigung ist für diesen S3-Bucket deaktiviert

Der zugehörige Status-Ursachencode lautet`EVENTBRIDGE_MANAGED_EVENTS_DELIVERY_DISABLED`.

Detail zum Status

GuardDuty verwendet EventBridge , um eine Benachrichtigung zu erhalten, wenn ein neues Objekt in diesen S3-Bucket hochgeladen wird. Diese Berechtigung fehlt in Ihrer IAM-Rolle.

Schritte zur Fehlerbehebung

Option 1: Fügen Sie Ihrer IAM-Rolle die folgende Berechtigungserklärung hinzu:

```
{
          "Sid": "AllowEnableS3EventBridgeEvents",
          "Effect": "Allow",
          "Action": [
             "s3:PutBucketNotification",
             "s3:GetBucketNotification"
             ],
          "Resource": [
             "arn:aws:s3:::amzn-s3-demo-bucket"
            ]
}
```

*amzn-s3-demo-bucket*Ersetzen Sie es durch Ihren Amazon S3 S3-Bucket-Namen.

Option 2: EventBridge Benachrichtigung mithilfe der Amazon S3 S3-Konsole aktivieren

1. Öffnen Sie die Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie auf der Seite Buckets auf der Registerkarte Allgemeine Buckets den Bucket-Namen aus, der mit diesem Fehler verknüpft ist.

3. Wählen Sie auf dieser Bucket-Seite die Registerkarte Eigenschaften aus.
4. Wählen Sie im EventBridge Bereich Amazon die Option Bearbeiten aus.
5. Wählen Sie auf der EventBridge Seite Amazon bearbeiten für Benachrichtigung an Amazon senden EventBridge für alle Ereignisse in diesem Bucket die Option An.
6. Wählen Sie Änderungen speichern aus.

Es kann einige Minuten dauern, bis der Wert in der Spalte Status auf Aktiv geändert wird.

EventBridge Eine verwaltete Regel zum Empfangen von S3-Bucket-Ereignissen fehlt

Der zugehörige Status-Ursachencode lautet`EVENTBRIDGE_MANAGED_RULE_DISABLED`.

Detail zum Status

Die EventBridge verwalteten Regelberechtigungen zur Verwaltung der EventBridge Regeleinrichtung fehlen.

Schritte zur Fehlerbehebung

Fügen Sie Ihrer IAM-Rolle die folgende Berechtigungserklärung hinzu:

```
{
         "Sid": "AllowManagedRuleToSendS3EventsToGuardDuty",
        "Effect": "Allow",
        "Action": [
                "events:PutRule",
                "events:DeleteRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
        "Resource": [
           "arn:aws:events:*:*:rule/DO-NOT-DELETE-
AmazonGuardDutyMalwareProtectionS3*"
           ],
        "Condition": {
           "StringEquals": {
              "events:ManagedBy": "malware-protection-plan.guardduty.amazonaws.com"
              }
           }
}
```

Es kann einige Minuten dauern, bis der Wert in der Spalte Status auf Aktiv geändert wird.

Der S3-Bucket ist nicht mehr vorhanden

Der zugehörige Status-Ursachencode lautet`PROTECTED_RESOURCE_DELETED`.

Detail zum Status

Dieser S3-Bucket wurde aus Ihrem Konto gelöscht und ist nicht mehr vorhanden.

Schritt zur Fehlerbehebung

Wenn das Löschen des S3-Buckets nicht beabsichtigt war, können Sie mithilfe der Amazon S3 S3-Konsole einen neuen Bucket erstellen.

Nachdem Sie den Bucket erfolgreich erstellt haben, aktivieren Sie den Malware-Schutz für S3, indem Sie die Schritte Konfiguration des Malware-Schutzes für S3 für Ihren Bucket auf der Seite befolgen.

Das Testobjekt konnte nicht platziert werden

Der zugehörige Status-Ursachencode lautet`INSUFFICIENT_TEST_OBJECT_PERMISSIONS`.

> **Note**
>
> Die Erlaubnis, ein Testobjekt hinzuzufügen, ist optional. Das Fehlen dieser Berechtigung in Ihrer IAM-Rolle verhindert nicht, dass Malware Protection for S3 einen Malware-Scan für ein neu hochgeladenes Objekt initiiert. Nach dem erfolgreichen Start eines Scans kann es einige Minuten dauern, bis der Status des Malware-Schutzplans von Warnung auf Aktiv geändert wird.
> Wenn die IAM-Rolle diese Berechtigung bereits beinhaltet, weist diese Warnung auf eine restriktive Amazon S3 S3-Bucket-Richtlinie hin, die es dem IAM-Zugriff nicht erlaubt, das Testobjekt in diesen S3-Bucket zu legen.

Einzelheiten zum Status

GuardDuty Fügt ein Testobjekt in Ihren Bucket ein, um die Einrichtung des ausgewählten Buckets zu überprüfen.

Schritte zur Fehlerbehebung

Sie können sich dafür entscheiden, die IAM-Rolle so zu aktualisieren, dass sie die fehlenden Berechtigungen einbezieht. Fügen Sie der ausgewählten IAM-Rolle die folgenden Berechtigungen hinzu, damit das Testobjekt der ausgewählten Ressource zugewiesen werden GuardDuty kann:

```
{
         "Sid": "AllowPutValidationObject",
         "Effect": "Allow",
         "Action": [
           "s3:PutObject"
           ],
         "Resource": [
           "arn:aws:s3:::amzn-s3-demo-bucket/malware-protection-resource-validation-
object"
           ]
}
```

*amzn-s3-demo-bucket*Ersetzen Sie es durch Ihren Amazon S3 S3-Bucket-Namen. Informationen zu IAM-Rollenberechtigungen finden Sie unterIAM-Rollenrichtlinie erstellen oder aktualisieren.

Es kann einige Minuten dauern, bis der Wert in der Spalte Status auf Aktiv geändert wird.

Problembehebung bei Malware-Scan auf Abruf

Ein Scan konnte nicht gestartet werden.

Bitte stellen Sie sicher, dass die Scananforderung gültige Eingaben enthält und der Malware-Schutzplan für den Bucket aktiviert ist.

Malware-Schutzplan für einen geschützten Bucket bearbeiten

Möglicherweise müssen Sie die bevorzugte IAM-Berechtigungsrichtlinie bearbeiten, das Tagging des gescannten S3-Objekts aktivieren oder deaktivieren oder S3-Objektpräfixe hinzufügen oder entfernen. Als Sie beispielsweise den Malware-Schutz für S3 für Ihren Bucket aktiviert haben, haben Sie entschieden, das Taggen des gescannten S3-Objekts mit dem Scanergebnis nicht zu aktivieren. Jetzt möchten GuardDuty Sie jedoch das vordefinierte Tag und das Scanergebnis als Tag-Wert hinzufügen.

Wählen Sie eine bevorzugte Zugriffsmethode, um den Malware-Schutzplan für Ihren geschützten S3-Bucket zu aktualisieren.

Console

Um einen Malware-Schutzplan zu bearbeiten

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich die Option Malware Protection for S3 aus.
3. Wählen Sie unter Geschützte Buckets den Bucket aus, für den Sie die bestehende Konfiguration bearbeiten möchten.
4. Wählen Sie Bearbeiten aus.
5. Aktualisieren Sie die bestehende Konfiguration und die Einstellungen für Ihren Bucket und bestätigen Sie die Änderungen. Informationen zur Beschreibung und zu den einzelnen Schritten für die einzelnen Abschnitte finden Sie unterMalware-Schutz für S3 für Ihren Bucket aktivieren.

   Überwachen Sie die Statusspalte für diesen geschützten Bucket. Wenn es entweder als Warnung oder als Fehler angezeigt wird, finden Sie weitere Informationen unterFehlerbehebung beim Status des Malware-Schutzplans.

API/CLI

Um den Malware-Schutzplan mithilfe der API zu bearbeiten oder AWS CLI

- Durch die Verwendung der API

  Führen Sie die UpdateMalwareProtectionPlanAPI mithilfe der mit dieser Planressource verknüpften Paket-ID für den Malware-Schutz aus.

  Um die ID des Malware-Schutzplans in einer bestimmten Region abzurufen, können Sie die ListMalwareProtectionPlansAPI in dieser Region ausführen.
- Durch die Verwendung von AWS CLI

  Die folgende Liste enthält AWS CLI Beispielbefehle zum Aktualisieren der Planressource für den Malware-Schutz. Sie benötigen die Ihrem S3-Bucket zugeordnete ID des Malware Protection-Plans.

AWS CLI Beispielbefehle

- Verwenden Sie den folgenden AWS CLI Befehl, um das Tagging für die Ressource des Malware-Schutzplans zu aktivieren oder zu deaktivieren, die Ihrem S3-Bucket zugeordnet ist:

```
aws guardduty update-malware-protection-plan --malware-protection-plan-
id 4cc8bf26c4d75EXAMPLE --actions "Tagging"={"Status"="ENABLED|DISABLED"}
```

- Verwenden Sie den folgenden AWS CLI Befehl, um der Ressource des Malware-Schutzplans, die Ihrem S3-Bucket zugeordnet ist, ein Objektpräfix hinzuzufügen:

```
aws guardduty update-malware-protection-plan --malware-
protection-plan-id 4cc8bf26c4d75EXAMPLE --protected-resource
 "S3Bucket"={"ObjectPrefixes"["amzn-s3-demo-1", "amzn-s3-demo-2"]}
```

  Stellen Sie sicher, dass Sie die vorhandenen Objektpräfixe in diesem Befehl angeben. Andernfalls GuardDuty werden diese Präfixe entfernt, wenn Sie die Ressource des Malware-Schutzplans bearbeiten.

- Verwenden Sie den folgenden AWS CLI Befehl, um ein Objektpräfix aus der Ressource des Malware-Schutzplans zu entfernen, die Ihrem S3-Bucket zugeordnet ist:

```
aws guardduty update-malware-protection-plan --malware-protection-plan-
id 4cc8bf26c4d75EXAMPLE --protected-resource "S3Bucket"={"ObjectPrefixes"[""]}
```

Wenn Sie noch nicht über die ID des Malware-Schutzplans für diese Ressource verfügen, können Sie den folgenden AWS CLI Befehl ausführen und ihn durch die Region *us-east-1* ersetzen, für die Sie die Kennungen des Malware-Schutzplans auflisten möchten.

```
aws guardduty list-malware-protection-plans --region us-east-1
```

Malware-Schutz für S3 für einen geschützten Bucket deaktivieren

Wenn Sie Malware Protection for S3 für einen geschützten Bucket deaktivieren, wird die diesem Bucket zugeordnete Plan-ID für den Schadsoftware-Schutz GuardDuty gelöscht. GuardDuty startet keinen Malware-Scan mehr, wenn ein neues Objekt in diesen Bucket oder eines der ausgewählten Objektpräfixe hochgeladen wird.

Wenn Sie die Option aktiviert haben GuardDuty und nun den Vorgang unterbrechen oder deaktivieren möchten GuardDuty, finden Sie weitere Informationen unterAussetzen oder Deaktivieren GuardDuty. Da es in Malware Protection for S3 kein Konzept für die Detektor-ID gibt, wirkt sich die Deaktivierung oder Sperrung GuardDuty nicht auf den Status eines geschützten Buckets in Ihrem Konto aus. Sie können die Funktion Malware Protection for S3 unabhängig weiter nutzen, wobei der entsprechende Standardpreis anfällt. Weitere Informationen finden Sie unter Überprüfung der Nutzungskosten für Malware Protection for S3. Um die Nutzung von Malware Protection for S3 zu beenden, müssen Sie ihn für alle geschützten Buckets in Ihrem Konto deaktivieren. Wenn Sie weiterhin nur Malware Protection for S3 für einen Bucket verwenden GuardDuty und deaktivieren möchten, wirken sich die folgenden Schritte nicht auf die Konfiguration des GuardDuty Dienstes und andere Schutzpläne aus, die Sie möglicherweise aktiviert haben.

Wählen Sie eine bevorzugte Zugriffsmethode, um Malware Protection for S3 in Ihrem geschützten S3-Bucket zu deaktivieren.

Console

So deaktivieren Sie den Malware-Schutz für S3 mithilfe der GuardDuty Konsole

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich die Option Malware Protection for S3 aus.
3. Wählen Sie unter Geschützte Buckets den Bucket aus, für den Sie Malware Protection for S3 deaktivieren möchten.

   Sie können jeweils nur einen geschützten Bucket auswählen. Um den Malware-Schutz für S3 für mehr als einen Bucket zu deaktivieren, führen Sie diese Schritte erneut für einen anderen S3-Bucket aus.
4. Wählen Sie Deaktivieren, um die Auswahl zu bestätigen.

API/CLI

Um den Malware-Schutz für S3 mithilfe der API zu deaktivieren oder AWS CLI

- Durch die Verwendung von API

  Führen Sie die DeleteMalwareProtectionPlanAPI mithilfe der mit dieser Planressource verknüpften Paket-ID für den Malware-Schutz aus.

Um die ID des Malware-Schutzplans abzurufen, können Sie die ListMalwareProtectionPlansAPI ausführen.

- Durch die Verwendung von AWS CLI

  Alternativ können Sie den folgenden AWS CLI Befehl ausführen, um den Malware-Schutz für S3 zu deaktivieren, indem Sie ihn *4cc8bf26c4d75EXAMPLE* durch die diesem S3-Bucket zugeordnete Plan-ID für den Schadsoftware-Schutz ersetzen:

  ```
  aws guardduty delete-malware-protection-plan --malware-protection-plan-
  id 4cc8bf26c4d75EXAMPLE
  ```

  Wenn Sie noch nicht über die ID des Malware-Schutzplans für diesen S3-Bucket verfügen, können Sie den folgenden AWS CLI Befehl ausführen und ihn durch die Region *us-east-1* ersetzen, für die Sie die Kennungen des Malware-Schutzplans auflisten möchten.

  ```
  aws guardduty list-malware-protection-plans --region us-east-1
  ```

Unterstützbarkeit der Amazon S3 S3-Funktionen

In der folgenden Tabelle wird angegeben, ob Malware Protection for S3 die aufgelisteten Amazon S3 S3-Funktionen unterstützt.

Ist der Support verfügbar?	Description
Ja	S3-Objekte können abgerufen werden, ohne dass sie asynchron wiederhergestellt werden müssen.

Ist der Support verfügbar?	Description

Ist der Support verfügbar?	Description
Bedingt	• Intelligent Tiering ist für S3-Objekte in den Stufen „Häufiger“, „Seltener Zugriff“ und „Archive-Instanzzu griff“ verfügbar. • Die Opt-in-Stufen Archive und Deep Archive werden nicht unterstützt. • Intelligent Tiering erstellt in der Stufe „Häufiger Zugriff“ immer ein neues Objekt. Daher wird der Objektscan bei der Erstellung unterstützt. • Künftige intelligente Tiering-Funktionen könnten zunächst Objekte im Archiv erstellen. Daher wird dies nicht unterstützt.
Nein	GuardDuty unterstützt nur Allzweck-Buckets für den Malware-Schutz für S3.

Ist der Support verfügbar?	Description
Nein	Die S3-Objekte müssen wiederhergestellt werden, bevor auf sie zugegriffen werden kann.
Nein	Der Malware-Schutz für S3 wird auf Outposts nicht unterstützt.
Ja	Alle hochgeladenen S3-Objekte werden auf Malware gescannt. Wenn Sie ein Objekt mit Dateiversion v1 hochgeladen haben und sofort eine weitere Versionsü berschreibung mit Version v2 hochgeladen haben, GuardDuty werden beide Objektdateiversionen v1 und v2 gescannt. Die Startzeit des Scans ist jedoch möglicher weise nicht in derselben Reihenfolge.

Ist der Support verfügbar?	Description
Ja	Wenn es sich bei dem Ziel-Bucket um eine geschützte Ressource handelt, GuardDuty werden alle S3-Objekte gescannt, die auf die geschützten und überwachten Präfixe repliziert wurden.
Nein	Sie können keine Replikationsregel auf der Grundlage des Scanergebnis-Tags definieren. Amazon S3 unterstützt keine Replikation für Tags, außer bei der Erstellung.

Ist der Support verfügbar?	Description
Ja	GuardDuty unterstützt Malware-Scans nach S3-Objekten, die mit verwalteten und vom Kunden verwalteten Schlüsseln verschlüsselt sind. Stellen Sie sicher, dass die IAM-Rolle die Berechtigung zur Verwendung des Schlüssels beinhaltet. Weitere Informationen finden Sie unter Hinzufügen von IAM-Richtlinienberechtigungen.

Ist der Support verfügbar?	Description
Nein	Malware Protection for S3 unterstützt nicht das Scannen von S3-Objekten, die mit Schlüsseln verschlüsselt sind, auf die nicht zugegriffen werden kann.
Nein	Wenn Ihre Amazon S3-Objekte mithilfe des Amazon S3 Encryption Client verschlüsselt werden, werden Ihre Objekte nicht an Dritte weitergegeben, auch nicht AWS. Informationen darüber, warum dies nicht unterstützt wird, finden Sie unter Schutz von Daten durch clientseitige Verschlüsselung. **Note** CSE-KMS verschlüsselte Objekte werden als verschlüsselter Blob empfangen, bei dem die Verschlüsselung nicht bestimmt werden kann. GuardDutyVerarbeitet sie daher so, wie sie empfangen werden, und scannt den verschlüs selten Blob als normale Datei. GuardDuty gibt keinen `UNSUPPORTED` Scanstatus für solche Objekte zurück, es sei denn, einer der Werte Kontingente im Malware-Schutz für S3 überschre itet den Status.

Ist der Support verfügbar?	Description
Ja	Gesperrte S3-Objekte werden auf der Grundlage von WORM — Write Once Read Many gesperrt. Malware Protection for S3 kann auf die Objekte zugreifen und sie scannen.
Ja	Malware Protection for S3 kann die Buckets scannen, die mit Requester Pays eingerichtet wurden. Der Anforderer zahlt für die S3-Anrufe. Weitere Informationen finden Sie unter Verwendung von Anforderer zahlt Buckets für Speicherübertragungen und -nutzung im Amazon-S3-Benutzerhandbuch.
Ja	Sie können Lebenszyklusrichtlinien auf der Grundlage des Scanergebnis-Tags definieren. Löschen Sie beispielsweise bösartige Objekte automatisch. Weitere Informationen zur Lebenszykluskonfiguration finden Sie unter Verwaltung Ihres Speicherlebenszyklus im Amazon S3 S3-Benutzerhandbuch.
Ja	Sie können Bucket-Ressourcenrichtlinien auf der Grundlage Ihres Ergebnis-Tags für den S3-Objektscan definieren. Verhindern Sie beispielsweise den Zugriff auf S3-Objekte, die noch nicht gescannt wurden, oder auf GuardDuty erkannte Bedrohungen. Weitere Informationen finden Sie unter Verwenden von tagbasierter Zugriffskontrolle (TBAC) mit Malware Protection for S3.

Ist der Support verfügbar?	Description
Nein	Malware Protection for S3 scannt nur den Inhalt des S3-Objekts.

Kontingente im Malware-Schutz für S3

Dieser Abschnitt enthält Standardkontingente, die oft als Grenzwerte bezeichnet werden. Sofern nicht anders angegeben, gilt jedes Kontingent Region-specific. Standardkontingente für die Nutzung des GuardDuty Basisdienstes finden Sie unterGuardDuty Amazon-Kontingente.

In den folgenden Tabellen werden die verschiedenen Kontingente beschrieben, die für Sie AWS-Konto gelten.

AWS Standardkontingentwert	Ist er einstellbar?	Description
100 GB	Nein	Die maximale S3-Objektgröße, mit der versucht GuardDuty wird, nach Malware zu suchen. Dieses Kontingent ist zwar nicht anpassbar, wenn Sie jedoch größere Objekte scannen müssen, wenden Sie sich an uns, AWS Support um zu erfahren, ob das Kontingent für Ihren Anwendungsfall erhöht werden GuardDuty kann.
100 000	Nein	Die maximale Anzahl von Dateien, die in einem S3-Objekt extrahiert und analysiert werden GuardDuty können.

AWS Standardkontingentwert	Ist er einstellbar?	Description
		Note Zusammengesetzte Dateitypen unterliegen möglicherweise diesen Beschränkungen. Zu den Dateitypen gehören, ohne darauf beschränkt zu sein, MIME-kodierte E-Mail-Nachrichten (Multipurpose Internet Mail Extensions), kompilierte Python-Dateien (PYC), kompilierte HTML-Hilfedateien (CHM), alle Installationsprogramme und OpenDocument Format- (ODF) -Dokumente. **Note** S3-Objekte mit einem extrem hohen Komprimierungsverhältnis zwischen der Größe des S3-Objekts und der Größe des extrahierten Inhalts können Beschränkungen unterliegen, selbst wenn die extrahierten Dateien dieses Kontingent unterschreiten.
100	Nein	Die maximalen Verschachtelungsebenen, die in einem S3-Objekt extrahiert werden GuardDuty können.

AWS Standardkontingentwert	Ist er einstellbar?	Description
25	Nein	Die maximale Anzahl von S3-Buckets, für die Sie Malware Protection for S3 aktivieren können. Diese Kontingentbegrenzung gilt pro Konto in jeder Region.

GuardDuty Malware-Schutz für AWS Backup

Topics

- -Übersicht
- Wie funktioniert der Malware-Schutz für Backups?
- GuardDuty Malware-Schutz für Backups: IAM-Rollenberechtigungen
- (Optional) Starten Sie eigenständig mit Malware Protection for Backup (nur Konsole)
- Einen On-Demand Scan zum Schutz vor Schadsoftware für Backups starten
- Überwachung des Scanstatus und der Ergebnisse in Malware Protection for Backup
- Kontingente für den Schutz vor Schadsoftware für Backups

-Übersicht

Malware Protection for Backup hilft Ihnen dabei, das potenzielle Vorhandensein von Malware in Ihren Backup-Daten zu erkennen, indem AWS Backup-geschützte Ressourcen wie Amazon EBS-Snapshots, Amazon EC2-AMIs und Amazon S3-Wiederherstellungspunkte gescannt werden. Wenn AWS Backup eine geschützte Backup-Ressource erstellt oder aktualisiert, GuardDuty kann für dieses Backup einen Malware-Scan durchführen, um potenziell schädliche Inhalte zu identifizieren, bevor sie in Ihrer Umgebung wiederhergestellt werden.

Wie können Sie den Malware-Schutz für Backups verwenden

Sie können diese Funktion in zwei Modi verwenden, je nachdem, ob sie in Ihrem Konto aktiviert GuardDuty ist:

1. Verwenden von Malware Protection for Backup bei GuardDuty aktiviertem

   Wenn die Option in einer Region aktiviert GuardDuty ist, integriert AWS Backup den Malware-Schutz in den GuardDuty Ermittlungsworkflow. Die Ergebnisse der Malware-Scans werden zusätzlich zu Amazon EventBridge und Amazon in den GuardDuty Ergebnissen angezeigt CloudWatch.
2. Verwenden Sie den Malware-Schutz für Backups, ohne ihn zu aktivieren GuardDuty

   Sie können Malware Protection for Backup unabhängig verwenden, ohne den vollen GuardDuty Service zu aktivieren. In diesem Modus bleiben die Scanergebnisse über EventBridge und vollständig verfügbar CloudWatch.

Überlegungen zur unabhängigen Verwendung von Malware Protection for Backup

Wenn Sie die Funktion verwenden, ohne sie zu aktivieren GuardDuty:

- Die Konfiguration des Backup-Plans wird vollständig in AWS Backup verwaltet.

GuardDuty bietet keine Steuerelemente für die Auswahl von Backup-Plänen, Tresoren oder Ressourcentypen. Alle Aktivierungs-, Zeitplanungs- und Richtlinienkonfigurationen verbleiben im Backup. AWS

- GuardDuty Ergebnisse werden nicht generiert.

Für Ergebnisse ist eine Detektor-ID erforderlich, die nur erstellt wird, wenn sie aktiviert GuardDuty ist. Wenn Sie den Malware-Schutz unabhängig verwenden, werden die Scanergebnisse ausschließlich anhand von EventBridge Ereignissen und CloudWatch Metriken angezeigt.

- Sie können weiterhin On-Demand-Scans von der GuardDuty Konsole aus starten.

Auch wenn die GuardDuty Konsole nicht aktiviert GuardDuty ist, bietet sie einen Workflow zum Starten eines On-Demand-Malware-Scans für unterstützte Backup-Ressourcentypen. Auf diese Weise können Kunden eine vertraute GuardDuty Oberfläche verwenden, ohne den vollen GuardDuty Service in Anspruch nehmen zu müssen.

- Non-GuardDuty Kunden können auf Workflows zur Scan-Initiierung zugreifen.

Die Einstiegspunkte für On-Demand-Scans stehen allen Kunden zur Verfügung, die Malware Protection for Backup verwenden, unabhängig davon, ob im Konto ein GuardDuty Detektor vorhanden ist.

- Scanverhalten und Reichweite bleiben identisch.

Unabhängig davon, ob die Funktion aktiviert GuardDuty ist oder nicht, scannt sie dieselben AWS Backup-Ressourcentypen mit derselben Malware-Erkennungsengine. Der einzige Unterschied besteht darin, wo die Ergebnisse veröffentlicht werden.

Dieses Modell ermöglicht es Kunden, Backups auf Schadsoftware zu scannen, ohne die GuardDuty umfassenderen Funktionen zur Bedrohungserkennung in Anspruch nehmen zu müssen, und bietet

gleichzeitig einen optionalen GuardDuty-based Arbeitsablauf für das Initiieren und Anzeigen von Scanvorgängen.

So funktioniert Malware Protection for Backup

Malware Protection for Backup kann die folgenden durch AWS Backups geschützten Ressourcen scannen:

- Amazon EBS snapshots
- Amazon EC2-AMIs
- Amazon S3-Wiederherstellungspunkte und kontinuierliche S3-Backups oder Point-in-Time-Recovery (PITR)
- Gesperrte (unveränderliche) Tresore (EBS/EC2 Recovery Points) mithilfe AWS von Backup Vault Lock in unterstützten Regionen https://docs.aws.amazon.com/aws-backup/latest/devguide/backup-feature-availability.html#features-by-region

Inkrementelles Scannen

AWS Backup erfasst inkrementelle Änderungen für viele Ressourcentypen. GuardDuty ist in der Lage, nur die neuen oder geänderten Blöcke oder Objekte zu scannen, wenn ein Backup erstellt oder aktualisiert wird. Dadurch wird die Leistung verbessert, der Scanaufwand reduziert und gleichzeitig im Laufe der Zeit eine vollständige Abdeckung erreicht.

On-demand scannen

Sie können jederzeit einen Scan auf jeder unterstützten Backup-Ressource starten — direkt von AWS Backup oder der GuardDuty Konsole aus. Zu den häufigsten Anwendungsfällen gehören die Überprüfung eines Backups vor der Wiederherstellung, die erneute Überprüfung älterer Daten nach der Veröffentlichung neuer Bedrohungssignaturen oder die Durchführung regelmäßiger Compliance-Scans.

> **Note**
>
> - Malware Protection for Backup kann nur für Backup-Ressourcen in derselben Region aktiviert werden.
> - GuardDuty scannt eine schreibgeschützte Kopie des Backups; der Inhalt des Backups wird dadurch nicht geändert.

- Das Scannen funktioniert sowohl für Standardtresoren als auch für gesperrte (unveränderliche) Tresore.

Wie funktioniert der Malware-Schutz für Backups?

In diesem Abschnitt werden die Komponenten von Malware Protection for Backup beschrieben, wie sie funktioniert und wie Sie den Status und das Ergebnis der Malware-Suche überprüfen können.

-Übersicht

Malware Protection for Backup ist eine Funktion, mit der Sie das Vorhandensein von Malware auf EBS-Snapshots, EC2-Images (AMI) und Recovery Points erkennen können, die zu den EBS-, EC2- und S3-Ressourcentypen gehören. Sie können einen On-Demand-Malware-Scan entweder über die GuardDuty Konsole oder die API starten, indem Sie eine IAM-Rolle, die die für den Scan erforderlichen Berechtigungen bereitstellt, zusammen mit einer oder zwei Ressourcen-ARNs, je nach Scan-Kategorie, übergeben. Es sind zwei Scan-Kategorien möglich: vollständige Scans und inkrementelle Scans.

Vollständiger Scan und Inkrementeller Scan

Bei einem vollständigen Scan akzeptiert die API einen Ressourcen-ARN und scannt alle Dateien in dieser Ressource. Ein inkrementeller Scan verwendet dagegen zwei Ressourcen-ARNs, die beide zu derselben Ressource gehören, und scannt die geänderten Dateien zwischen ihnen. Nehmen wir als Beispiel an, wir erstellen einen Snapshot eines EBS-Volumes. Nennen wir es Snapshot-1. Wenn dieser Snapshot vollständig gescannt wird, werden alle in diesem Snapshot enthaltenen Dateien GuardDuty gescannt. Nehmen wir nun an, dass ein paar Dateien demselben Volume hinzugefügt wurden und ein neuer Snapshot erstellt wird. Nennen wir es Snapshot-2. Da sich nur wenige Dateien zwischen Snapshot-1 und Snapshot-2 geändert haben, kann man einen inkrementellen Scan mit den Ressourcen-ARNs dieser beiden Snapshots auslösen. In diesem Fall wird Snapshot-2 als Ressource und Snapshot-1 als Ressource bezeichnet. `target base` Sie werden sehen, dass diese Terminologie im Rest des Dokuments verwendet wird. Bei diesem inkrementellen Scan werden die zwischen Schnappschuss-1 und Schnappschuss-2 geänderten Dateien gescannt.

Suche nach Point-in-Time-Recovery Schadsoftware nach (PITR)

Wenn diese Option im AWS Backup aktiviert ist, erfolgt die Malware-Suche nach kontinuierlichen Backups oder PITR entsprechend der im Backup-Plan konfigurierten Häufigkeit. Dies wird vom AWS

Backup-Dienst orchestriert. Führt beispielsweise GuardDuty den ersten Scan von t0 nach t2 aus, den nächsten Scan von t2 nach t4, den nachfolgenden Scan von t4 nach t6 usw. Jeder dieser Scans generiert eine Scan-ID, die mithilfe der `GetMalwareScan` API abgefragt werden kann, um den Status und das Ergebnis des Scans für diesen Zeitraum abzurufen.

Alternativ können Sie auch die gesamte PITR-Ressource von der GuardDuty Konsole aus scannen oder die GuardDuty `StartMalwareScan` API bei Bedarf verwenden, indem Sie einen Endzeitstempel übergeben. Dadurch wird sichergestellt, dass die gesamte Ressource vom Anfang bis zum Endzeitstempel GuardDuty gescannt wird.

> **Note**
>
> - Sie können keine teilweisen oder inkrementellen Scans auf PITR von auslösen. GuardDuty
> - Der für einen Scan auf Anforderung übergebene Endzeitstempel darf nicht älter sein als (aktuelle Uhrzeit: 15 Minuten).

Erneutes Scannen zuvor infizierter Dateien in einem inkrementellen Scan

Im Rahmen eines inkrementellen Scans GuardDuty werden auch die zuvor infizierten Dateien aus dem Basis-Scan bis zu 365 Tage lang erneut gescannt.

Voraussetzungen für einen inkrementellen Scan

Die folgenden Anforderungen müssen erfüllt sein, GuardDuty um einen inkrementellen Scan durchführen zu können. Wenn eine dieser Anforderungen nicht erfüllt ist, GuardDuty wird der Scan übersprungen.

- Die Basisressource muss innerhalb der letzten 365 Tage gescannt worden sein und das Scanergebnis muss in `COMPLETED` oder stehen`COMPLETED_WITH_ISSUES`.
- Die Basisressource muss ein Erstellungsdatum haben, das vor dem der Zielressource liegt.
- Bei Snapshots müssen die Basis- und Zielressourcen den gleichen Verschlüsselungstyp haben.
- Die Basis- und Zielressourcen müssen aus derselben Herkunft stammen.
  - Für einen EBS-Snapshot und einen EBS-Wiederherstellungspunkt bedeutet dies, dass sie entweder von demselben Volume oder von Kopien desselben Volumes stammen, ohne dass sich der Verschlüsselungstyp ändert.

- Für einen S3-Wiederherstellungspunkt müssen die Basis- und Zielressourcen-ARNs aus demselben zugrunde liegenden S3-Bucket erstellt werden.
- Bei AMIs werden Snapshot-Paare zwischen dem Basis- und dem Ziel-AMI verglichen, um Snapshots für einen inkrementellen Scan zu identifizieren. Jedes Snapshot-Paar muss die oben genannten Bedingungen erfüllen. Jeder Snapshot innerhalb des Ziel-AMI, der keinen entsprechenden passenden Snapshot im Basis-AMI hat, wird übersprungen.

Re-scanning zuvor gescannte Backup-Ressourcen

Sie können 10 Minuten nach der Startzeit des vorherigen Malware-Scans einen neuen On-Demand-Malware-Scan auf derselben Ressource starten. Wenn der neue Malware-Scan innerhalb von 10 Minuten nach dem Start des vorherigen Malware-Scans gestartet wird, führt Ihre Anfrage zu dem folgenden Fehler, und für diese Anfrage wird keine Scan-ID generiert. Die Schritte zum erneuten Scannen der Instanz bleiben dieselben wie beim ersten Starten eines On-Demand-Malware-Scans.

Für das Scannen ist eine IAM-Rolle erforderlich

Sie müssen eine IAM-Rolle übergeben, um einen vollständigen oder inkrementellen Scan zu starten. Diese Rolle bietet die für die Durchführung der Scanvorgänge erforderlichen Berechtigungen. GuardDuty Malware-Schutz für Backups: IAM-Rollenberechtigungenenthält die genaue Liste der erforderlichen Berechtigungen sowie die entsprechende Vertrauensrichtlinie, die für die Durchführung des Scans erforderlich ist.

Status und Ergebnis des Ressourcenscans werden überprüft

GuardDuty veröffentlicht das Ereignis mit dem Scanergebnis auf dem EventBridge Standard-Event-Bus von Amazon. GuardDuty verwendet die Übertragung mindestens einmal, was bedeutet, dass Sie möglicherweise mehrere Scanergebnisse für dasselbe Objekt erhalten. Wir empfehlen, Ihre Anwendungen so zu gestalten, dass doppelte Ergebnisse verarbeitet werden. Für jedes gescannte Objekt wird Ihnen nur einmal eine Rechnung gestellt.

Weitere Informationen finden Sie unter Überwachung des Scanstatus und der Ergebnisse in Malware Protection for Backup.

Überprüfung der generierten Ergebnisse

Die Überprüfung der Ergebnisse hängt davon ab, ob Sie Malware Protection for Backup mit verwenden oder nicht GuardDuty. Betrachten Sie folgende Szenarien:

Verwenden Sie Malware Protection for Backup, wenn Sie den GuardDuty Dienst aktiviert haben (Detektor-ID)

Wenn der Malware-Scan eine potenziell schädliche Datei in einer gescannten Backup-Ressource entdeckt, GuardDuty wird ein entsprechender Befund generiert. Sie können sich die Einzelheiten des Befundes ansehen und die empfohlenen Schritte ausführen, um den Befund möglicherweise zu korrigieren. Je nachdem, wie häufig Ihre Ergebnisse exportiert werden, wird das generierte Ergebnis in einen S3-Bucket und einen EventBridge Amazon-Event-Bus exportiert.

Informationen über den Findetyp, der generiert werden würde, Malware-Schutz für Backup-Suchtypen finden Sie unter Suchen nach Typen für Malware Protection for Backup.

Verwendung von Malware Protection for Backup als eigenständige Funktion (keine Detektor-ID)

GuardDuty kann keine Ergebnisse generieren, da keine zugehörige Detektor-ID vorhanden ist. Um den Scanstatus Ihrer Backup-Ressource zu erfahren, können Sie sich das Scan-Ergebnis ansehen, das GuardDuty automatisch auf Ihrem Standard-Event-Bus veröffentlicht wird.

Informationen zum Scanstatus und zum Ergebnis finden Sie unterÜberwachung des Scanstatus und der Ergebnisse in Malware Protection for Backup.

> **Note**
>
> Wenn Sie auch Malware Protection for S3 verwenden, besteht die Möglichkeit, dass Ihre S3-Datei zuvor als NO_THREATS_FOUND markiert wurde und dennoch dieselbe Datei in der Liste der Bedrohungen für den Backup Recovery Point auftaucht, zu dem das Objekt gehört. Dies ist darauf zurückzuführen, dass der Dienst seine Malware-Signaturen häufig aktualisiert, wodurch sich möglicherweise der Status der Datei geändert hat. Bitte beachten Sie, dass in solchen Fällen GuardDuty das Tag auf der Datei im ursprünglichen S3-Bucket nicht aktualisiert wird. Die einzige Möglichkeit, ein aktualisiertes Tag auf die Datei anzuwenden, besteht darin, das Objekt erneut in den Bucket hochzuladen oder die On-Demand-Scanfunktion für S3 zu verwenden.

GuardDuty Malware-Schutz für Backups: IAM-Rollenberechtigungen

Für das Scannen von Schadsoftware ist eine Kundenrolle vorgesehen

GuardDuty Malware Protection geht davon aus, dass beim Scannen von Backup-Ressourcen, d. h. Snapshots, AMIs und EBS/EC2/S3 Wiederherstellungspunkten, eine Kundenrolle (Scanner-Rolle) zugewiesen wird. Diese Rolle bietet die Berechtigungen, die für die GuardDuty Durchführung des Scans auf diesen spezifischen Ressourcen erforderlich sind. Die Berechtigungsrichtlinie und die Vertrauensrichtlinie für diese Rolle finden Sie unterBerechtigungen und Vertrauensrichtlinien für die Rolle. Im folgenden Abschnitt wird beschrieben, warum jede dieser Berechtigungen erforderlich ist.

Einzelheiten zu den Berechtigungen

- `ModifySnapshotAttribute`- Ermöglicht den Zugriff auf unverschlüsselte und vom Kunden verwaltete, durch Schlüssel verschlüsselte Snapshots über das GuardDuty Malware Protection-Dienstkonto.
- `CreateGrant`- Ermöglicht GuardDuty Malware Protection, über den vom Kunden verwalteten, verschlüsselten Snapshot, auf den das GuardDuty Dienstkonto Zugriff hat, ein vom Kunden verwaltetes, verschlüsseltes EBS-Volume zu erstellen und darauf zuzugreifen.
- `RetireGrant`- Ermöglicht es GuardDuty Malware Protection, die mit dem vom Kunden verwalteten Schlüssel gewährten Berechtigungen für das Lesen verschlüsselter Snapshots zurückzuziehen
- `ReEncryptTo`und `ReEncryptFrom` — Wird von EBS benötigt, um GuardDuty Zugriff auf Snapshots zu gewähren, die mit vom Kunden verwalteten Schlüsseln verschlüsselt sind, und um daraus verschlüsselte Volumes zu erstellen. Auch wenn Kunden einen Snapshot während ReEncryption der gemeinsamen Nutzung als wichtigen Übergang betrachten, bleiben Snapshots aus Kundensicht unveränderlich, sobald sie erstellt wurden.
- `ListSnapshotBlocks`und `GetSnapshotBlock` — EBS Direct-APIs werden verwendet, um auf die Snapshot-Blöcke für einen mit AWS Managed Key verschlüsselten Snapshot zuzugreifen. Dies geschieht, weil auf verschlüsselte Snapshots mit AWS Managed Key sonst nicht kontoübergreifend zugegriffen werden kann.
- `Decrypt`- Ermöglicht die Entschlüsselung von Basis-Snapshots, bei denen vom Kunden verwaltete Schlüssel verschlüsselt werden, wenn sie mithilfe der EBS Direct-APIs im Rahmen eines inkrementellen Scannens in den Speicher heruntergeladen werden.

- `ListChangedBlocks`- Die EBS Direct-API wird beim inkrementellen Snapshot-Scannen verwendet, um die Liste der geänderten Blöcke zwischen zwei Snapshots abzurufen.
- `DescribeKey`- Ermöglicht GuardDuty Malware Protection, die KeyID des AWS verwalteten Schlüssels im Kundenkonto zu ermitteln.
- `DescribeImages`- Ermöglicht die Beschreibung eines AMI, um die Liste der zum AMI gehörenden Snapshots abzurufen.
- `DescribeRecoveryPoint`- Ermöglicht dem Dienst, die Wiederherstellungspunktdetails abzurufen und den Ressourcentyp für den Recovery Point zu überprüfen.
- `CreateBackupAccessPoint`,`DescribeBackupAccessPoint`, `DeleteBackupAccessPoint` - Ermöglicht dem Dienst, den Access Point zu erstellen, zu beschreiben und zu löschen, der für den Zugriff auf Recovery Points erforderlich ist.
- `kms:Decrypt`- Ermöglicht dem Dienst den Zugriff auf Objekte in einem S3 Recovery Point während eines S3 Recovery Point-Scans.

Sicherung der Rolle

Die Rolle muss mit einer Vertrauensrichtlinie konfiguriert werden, die dem GuardDuty Malware Protection-Dienstprinzipal vertraut. Dadurch wird sichergestellt, dass kein anderer Principal als der GuardDuty Service diese Rolle übernehmen kann. Darüber hinaus wird empfohlen, die Richtlinien auf bestimmte Ressourcen zu beschränken, anstatt * Dazu gehören Snapshot-IDs und Schlüssel-IDs. Dadurch wird sichergestellt, dass die Rolle nur Zugriff auf diese spezifischen Ressourcen gewährt.

> **Important**
>
> Eine falsche Konfiguration kann aufgrund unzureichender Berechtigungen zu Scanfehlern führen.

So verwendet der GuardDuty Malware-Schutz Zuschüsse in AWS KMS

GuardDuty Für den Malware-Schutz sind Zuschüsse erforderlich, um Ihre KMS-Schlüssel verwenden zu können.

Wenn Sie einen Scan für einen verschlüsselten Snapshot oder ein EC2-AMI starten, das aus verschlüsselten Snapshots besteht, erstellt GuardDuty Malware Protection in Ihrem Namen

Zuschüsse, indem es eine CreateGrant Anfrage an AWS KMS sendet. Diese Zuschüsse ermöglichen GuardDuty den Zugriff auf einen bestimmten Schlüssel in Ihrem Konto.

GuardDuty Für den Schutz vor Schadsoftware ist der Zuschuss erforderlich, um Ihren vom Kunden verwalteten Schlüssel für die folgenden internen Vorgänge zu verwenden:

- Senden Sie DescribeKey Anfragen an AWS , um Details über den symmetrischen, vom Kunden verwalteten Schlüssel abzurufen, mit dem die für einen Malware-Scan übermittelte Ressource verschlüsselt ist.
- Erstellen Sie mithilfe der CreateVolume API ein EBS-Volume aus einem verschlüsselten Snapshot und verschlüsseln Sie das Volume mit demselben Schlüssel.
- Greifen Sie während eines inkrementellen Scans über die GetSnapshotBlock API auf Snapshot-Blöcke im Snapshot zu.
- Senden Sie https://docs.aws.amazon.com/kms/latest/APIReference/API_Decrypt.html Entschlüsselungsanfragen an AWS KMS, um die verschlüsselten Datenschlüssel zu entschlüsseln, sodass sie während des Scans zum Lesen der Daten im Snapshot verwendet werden können.

Sie können den gewährten Zuschuss jederzeit widerrufen oder dem Dienst den Zugriff auf den vom Kunden verwalteten Schlüssel entziehen. Wenn Sie dies tun, können Sie auf GuardDuty keine der Daten zugreifen, die mit dem vom Kunden verwalteten Schlüssel verschlüsselt wurden. Dies wirkt sich auf Vorgänge aus, die von diesen Daten abhängig sind.

GuardDuty Schutz vor Schadsoftware, Verschlüsselungskontext

Ein Verschlüsselungskontext ist ein optionaler Satz von Schlüssel-Wert-Paaren, die zusätzliche kontextbezogene Informationen zu den Daten enthalten.

Wenn Sie einen Verschlüsselungskontext in eine Anforderung zum Verschlüsseln von Daten einbeziehen, bindet AWS KMS; den Verschlüsselungskontext an die verschlüsselten Daten. Zur Entschlüsselung von Daten müssen Sie denselben Verschlüsselungskontext in der Anfrage übergeben.

GuardDuty Der Malware-Schutz verwendet einen der beiden Verschlüsselungskontexte.

Verschlüsselungskontext 1: Der Schlüssel ist`aws:guardduty:id`.

```
"encryptionContext": {
    "aws:guardduty:id": "snap-11112222333344"
```

```
}
```

Dieser Verschlüsselungskontext wird bei Gewährungsvorgängen verwendet: CreateGrant, Entschlüsseln GenerateDataKeyWithoutPlaintext,, ReEncryptTo RetireGrant, DescribeKey.

Ein Zuschuss wird für die aktuelle Ressource mit diesem Verschlüsselungskontext und diesen Gewährungsvorgängen erstellt.

Verschlüsselungskontext 2: Der Schlüssel ist `aws:ebs:id`

```
"encryptionContext": {
    "aws:ebs:id": "snap-11112222333344"
}
```

Dieser Verschlüsselungskontext wird bei Gewährungsvorgängen verwendet: ReEncryptFrom, Entschlüsseln, RetireGrant, DescribeKey.

Mit diesen Verschlüsselungskontexten und Gewährungsvorgängen werden drei Zuschüsse erstellt. Einer auf dem Ziel-Snapshot mit dem `ReEncryptFrom` Grant-Vorgang. Ein zweiter auf dem Ziel-Snapshot mit `Decrypt, RetireGrant, DescribeKey` Vorgängen. Und ein dritter auf dem Basis-Snapshot mit den gleichen Zuschussoperationen wie beim zweiten Zuschuss.

Berechtigungen und Vertrauensrichtlinien für die Rolle

Richtlinien für Berechtigungen

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ebs:GetSnapshotBlock"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*"
        },
        {
            "Sid": "CreateGrantPermissions",
            "Effect": "Allow",
            "Action": "kms:CreateGrant",
            "Resource": "arn:aws:kms:*:*:key/*",
```

```
            "Condition": {
                "ForAnyValue:StringLike": {
                    "kms:EncryptionContext:aws:guardduty:id": "snap-*",
                    "kms:ViaService": [
                        "guardduty.*.amazonaws.com",
                        "backup.*.amazonaws.com"
                    ]
                },
                "ForAllValues:StringEquals": {
                    "kms:GrantOperations": [
                        "Decrypt",
                        "CreateGrant",
                        "GenerateDataKeyWithoutPlaintext",
                        "ReEncryptFrom",
                        "ReEncryptTo",
                        "RetireGrant",
                        "DescribeKey"
                    ]
                },
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
            }
        },
        {
            "Sid": "CreateGrantPermissionsForReEncryptAndDirectAPIs",
            "Effect": "Allow",
            "Action": "kms:CreateGrant",
            "Resource": "arn:aws:kms:*:*:key/*",
            "Condition": {
                "ForAnyValue:StringLike": {
                    "kms:EncryptionContext:aws:ebs:id": "snap-*",
                    "kms:ViaService": [
                        "guardduty.*.amazonaws.com",
                        "backup.*.amazonaws.com"
                    ]
                },
                "ForAllValues:StringEquals": {
                    "kms:GrantOperations": [
                        "Decrypt",
                        "ReEncryptTo",
                        "ReEncryptFrom",
                        "RetireGrant",
                        "DescribeKey"
```

```
                ]
            },
            "Bool": {
                "kms:GrantIsForAWSResource": "true"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeImages",
            "ec2:DescribeSnapshots"
        ],
        "Resource": "*"
    },
    {
        "Sid": "ShareSnapshotPermission",
        "Effect": "Allow",
        "Action": [
            "ec2:ModifySnapshotAttribute"
        ],
        "Resource": "arn:aws:ec2:*:*:snapshot/*"
    },
    {
        "Sid": "ShareSnapshotKMSPermission",
        "Effect": "Allow",
        "Action": [
            "kms:ReEncryptTo",
            "kms:ReEncryptFrom"
        ],
        "Resource": "arn:aws:kms:*:*:key/*",
        "Condition": {
            "StringLike": {
                "kms:ViaService": "ec2.*.amazonaws.com"
            }
        }
    },
    {
        "Sid": "DescribeKeyPermission",
        "Effect": "Allow",
        "Action": "kms:DescribeKey",
        "Resource": "arn:aws:kms:*:*:key/*"
    },
    {
```

```
            "Sid": "DescribeRecoveryPointPermission",
            "Effect": "Allow",
            "Action": [
                "backup:DescribeRecoveryPoint"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateBackupAccessPointPermissions",
            "Effect" : "Allow",
            "Action" : [
                "backup:CreateBackupAccessPoint"
            ],
            "Resource": "arn:aws:backup:*:*:recovery-point:*"
        },
        {
            "Sid": "ReadAndDeleteBackupAccessPointPermissions",
            "Effect" : "Allow",
            "Action" : [
                "backup:DescribeBackupAccessPoint",
                "backup:DeleteBackupAccessPoint"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KMSKeyPermissionsForInstantAccess",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:*:*:key/*",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": "backup.*.amazonaws.com"
                }
            }
        }
    ]
}
```

Vertrauensrichtlinie

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

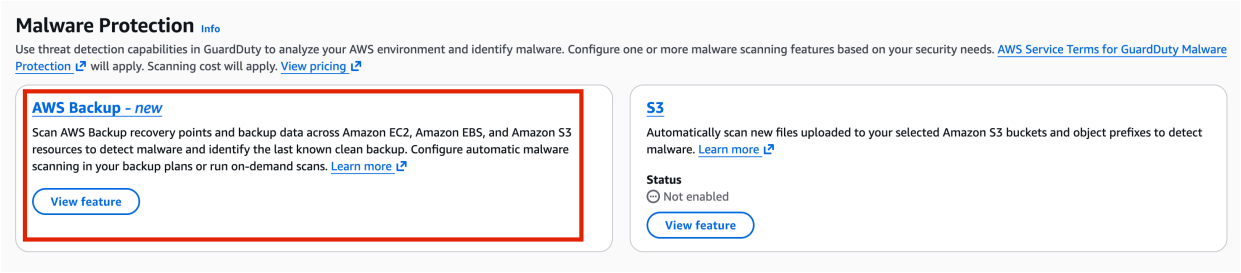
(Optional) Starten Sie eigenständig mit Malware Protection for Backup (nur Konsole)

Verwenden Sie diesen optionalen Schritt, wenn Sie unabhängig vom GuardDuty Status in Ihrem AWS Konto mit der Option zur Erkennung von Bedrohungen durch Malware Protection for Backup beginnen möchten.

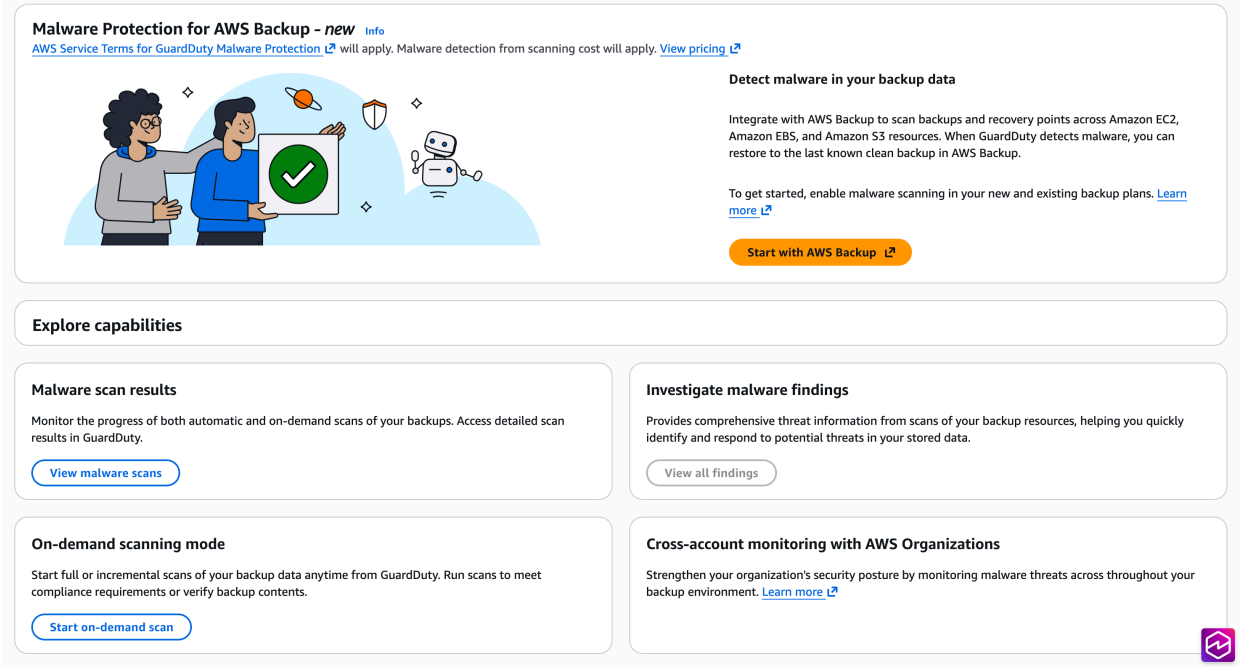
Wenn Sie auch andere spezielle Schutzpläne nutzen möchten GuardDuty, müssen Sie mit dem GuardDuty Amazon-Service beginnen. Informationen zu GuardDuty Schutzplänen finden Sie unter Funktionen von GuardDuty.

Schritte für die ersten Schritte mit Malware Protection for Backup

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die https://console.aws.amazon.com/guardduty/ Konsole unter https://console.aws.amazon.com/guardduty/
2. Wählen Sie Discover Malware Protection Features aus und klicken Sie auf Get Started.
3. Wenn Sie auf Erste Schritte klicken, können Sie zwischen Optionen wie den Funktionen AWS Backup und S3 Malware Protection wählen.



4. Sie werden zur Seite „Malware-Schutz für Backup“ weitergeleitet, auf der Sie wählen können, ob Sie einen Scan auf Anforderung starten oder Malware-Scans anzeigen möchten.



Einen On-Demand Scan zum Schutz vor Schadsoftware für Backups starten

Konsole

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Navigieren Sie zu Malware Protection for Backup und klicken Sie auf Scan auf Anforderung starten.
3. Wählen Sie zwischen Vollständiger Scan und Inkrementeller Scan.
    1. Um einen vollständigen Scan zu starten, geben Sie den Ressourcen-ARN der zu scannenden Ressource ein.
    2. Für einen inkrementellen Scan geben Sie den Zielressourcen-ARN und den Baseline-Ressourcen-ARN ein.
    3. Wenn es sich bei der zu scannenden Ressource um einen Recovery Point handelt, müssen Sie auch den Namen des AWS Backup-Tresors eingeben, zu dem er gehört.

4. Übergeben Sie für eine S3 PITR-Ressource einen Endzeitstempel. Der Endzeitstempel darf nicht älter sein als (aktuelle Zeit - 15 Minuten).

4. Servicezugriff — Sie müssen eine Rolle auswählen, die über die erforderlichen Berechtigungen für den Zugriff auf die Ressource und die Durchführung des Scans verfügt. Klicken Sie auf Richtlinie anzeigen, um die genauen Berechtigungen, die für die Rolle erforderlich sind, zusammen mit der erforderlichen Vertrauensrichtlinie anzuzeigen.

Sie können die Richtlinie je nach Ihren Anforderungen ändern oder die Berechtigungen auf die exakte Ressource beschränken. Weitere Informationen darüber, wie Sie eine IAM-Rolle erstellen oder aktualisieren können, finden Sie unterGuardDuty Malware-Schutz für Backups: IAM-Rollenberechtigungen.

Informationen zu Problemen mit IAM-Rollenberechtigungen finden Sie unter Problembehandlung bei IAM-Rollenberechtigungen.

API/CLI

Aufrufen StartMalwareScan, der den Wert `resourceArn` der Ressource akzeptiert, für die Sie einen On-Demand-Malware-Scan starten möchten. Wenn Sie einen inkrementellen Scan starten möchten, geben Sie das `baselineResourceArn` ein. `incrementalScanDetails` Im Rahmen der Scankonfiguration müssen Sie auch eine IAM-Rolle angeben, die über alle zum Starten des Scans erforderlichen Berechtigungen verfügt. Wenn es sich bei der gescannten Ressource um eine S3-PITR-Ressource handelt, müssen Sie einen Endzeitstempel übergeben. Nachdem Sie einen Scan erfolgreich gestartet haben, wird ein `StartMalwareScan` zurückgegeben. `scanId` Rufen Sie die `GetMalwareScan` API auf, um den Fortschritt des gestarteten Scans zu überwachen und Details zum Scan abzurufen, sobald er abgeschlossen ist.

Überwachung des Scanstatus und der Ergebnisse in Malware Protection for Backup

GuardDuty Stellt nach dem Initiieren eines Malware-Scans einige Mechanismen zur Verfügung, mit denen Sie den Status und das Ergebnis eines Scans überwachen können. Die folgende Tabelle enthält einige der Werte, die mit Malware-Scans verknüpft sind.

Mögliche Werte
`RUNNING`, `COMPLETED` , `COMPLETED_WITH_ISSUES` , `FAILED` oder `SKIPPED`
`FULL_SCAN` oder `INCREMENTAL_SCAN`
`GUARDDUTY_INITIATED` , `ON_DEMAND` oder `BACKUP_INITIATED`
`NO_THREATS_FOUND` oder `THREATS_FOUND`

*Beachten Sie, dass der Scan-Ergebnisstatus möglicherweise nicht angezeigt wird, wenn der Scan nicht abgeschlossen wurde. Der Scan-Ergebnisstatus von THREATS_FOUND gibt an, dass das Vorhandensein von Malware GuardDuty erkannt wurde.

Bei S3-Wiederherstellungspunkten gibt COMPLETED_WITH_ISSUES an, dass einige Dateien entweder übersprungen wurden oder fehlgeschlagen sind. Bei AMIs gibt COMPLETED_WITH_ISSUES an, dass mindestens ein Snapshot nicht gescannt werden konnte. Unten finden Sie eine Liste der Gründe, die übersprungen wurden.

Scans können aus verschiedenen Gründen auch übersprungen werden. In der folgenden Tabelle werden die Gründe erklärt, warum Scans übersprungen werden können:

Grund
Customer Role verfügt nicht über die erforderlichen Berechtigungen, damit der Service den Scan durchführen kann
Die Ressource, die gescannt werden soll, ist im Konto nicht vorhanden oder wurde während des Scannens gelöscht
Die Snapshot-Größe ist größer als derzeit unterstützt von GuardDuty
Die in der inkrementellen Scananforderung angegebenen Ressourcen unterscheiden sich nicht
Die Ressource befindet sich nicht im erwarteten Zustand. Wenn der Scan inkrementell ist, befindet sich der Basiswiederherstellungspunkt nicht im Status VERFÜGBAR oder ABGESCHLOSSEN
Für inkrementelle Scans: Die Basis- und die aktuelle Ressource stammen nicht aus derselben Herkunft
Bei inkrementellen Scans: Die Basisressource wurde zuvor nicht gescannt oder es wurde kein abgeschlossener Scan gefunden

Grund
Bei inkrementellen Scans: Das Erstellungsdatum der Basisressource ist größer als das Erstellungsdatum der aktuellen Ressource
Der angeforderte Ressourcentyp unterstützt kein inkrementelles Scannen
Öffentliche AMIs, AMIs mit nur flüchtigem Speicher und AMIs, die sich nicht in einem verfügbaren Status befinden, kommen nicht zum Scannen infrage
Cold Storage-Snapshots können nicht gescannt werden
Das Scannen wird für zusammengesetzte Ressourcentypen nicht unterstützt
Die angeforderte Ressource enthält einen Amazon Marketplace-Produktcode, der das Scannen nicht unterstützt
AMIs unterstützen das Scannen von mehr als 40 Schnappschüssen nicht
Für die angeforderte Ressource wurden keine Ebs-Blockgerätezuordnungen gefunden

Grund
Bei inkrementellen Scans unterscheidet sich der ARN der Basisressource vom ARN der erwartete n Ressource
Alle Dateien im Scan wurden entweder übersprungen oder sind fehlgeschlagen

Die Scanergebnisse haben eine Aufbewahrungsfrist von 90 Tagen. Wählen Sie Ihre bevorzugte Zugriffsmethode, um den Status Ihres Malware-Scans zu verfolgen.

Überwachen von Scans mithilfe der Konsole

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Malware-Scans.
3. Sie können die Malware-Scans anhand der folgenden Eigenschaften filtern, die in der Filter-Suchleiste verfügbar sind.

   - Scan-ID — Eindeutige Kennung, die dem Malware-Scan zugeordnet ist.
   - Konto-ID — Konto, auf dem der Malware-Scan initiiert wurde.
   - Ressourcen-ARN — Amazon-Ressourcenname (ARN), der der Amazon-Ressource zugeordnet ist, die mit dem Scan verknüpft ist.
   - Ressourcentyp — Der Ressourcentyp, der dem Scan zugeordnet ist, z. B. EC2-Instance, EBS Snapshot | EC2 AMI, EBS Recovery Point, EC2 Recovery Point oder S3 Recovery Point.
   - Status — Der Scanstatus des Scans, z. B. Wird ausgeführt, Übersprungen, Abgeschlossen, Mit Problemen abgeschlossen oder Fehlgeschlagen.
   - Scan-Typ — Gibt an, ob es sich um einen On-demand Scan oder einen Backup-Initiated Malware-Scan handelte. GuardDuty-initiated

Überwachung von Scans mit dem API/CLI

- Sie können aufrufen ListMalwareScans , um Malware-Scans nachRESOURCE_ARN,SCAN_ID, ACCOUNT_ID SCAN_TYPE GUARDDUTY_FINDING_ID SCAN_STATUSRESOURCE_TYPE, und SCAN_START_TIME zu filtern. Sie können auch aufrufen GetMalwareScan , um detailliertere Metadaten eines Scans abzurufen, indem Sie eine Scan-ID als Eingabe angeben. Die GUARDDUTY_FINDING_ID Filterkriterien sind verfügbar, wenn der SCAN_TYPE initiiert wird. GuardDuty
- Sie können das Beispiel *filter-criteria* im folgenden Befehl ändern und CriterionKey nacheinander filtern. Die Optionen für CriterionKey sind Resource_ARNSCAN_ID,ACCOUNT_ID,SCAN_TYPE, GUARDDUTY_FINDING_IDSCAN_STATUS,RESOURCE_TYPE, undSCAN_START_TIME. Sie können die *max-results* (bis zu 50) und die ändern*sort-criteria*. Das AttributeName Feld ist ein Pflichtfeld für sort-criteria und muss auf gesetzt werdenscanStartTime. Im folgenden Beispiel *red* sind die Werte in Platzhalter. Ersetzen Sie sie durch die für Ihr Konto geeigneten Werte. Wenn Sie dasselbe CriterionKey wie unten für verwenden, stellen Sie sicher ListMalwareScans, dass Sie das Beispiel EqualsValue durch das Beispiel ersetzen, nach dem *resource-type* Sie filtern möchten.

```
aws guardduty list-malware-scans --max-results 25 --sort-criteria
 '{"AttributeName": "scanStartTime", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"RESOURCE_TYPE", "FilterCondition":
{"EqualsValue":"EBS_SNAPSHOT"}}] }'
```

```
aws guardduty get-malware-scan --scan-id abc123
```

- Die Antwort auf den obigen Befehl für ListMalwareScans gibt bis zu 25 Scans mit einigen Details zu den betroffenen Ressourcen zurück. Die Antwort auf den obigen Befehl für GetMalwareScan gibt einen einzelnen Scan mit detaillierten Metadaten über den Scan zurück.

Überwachen von Scans mit EventBridge

Amazon EventBridge ist ein serverloser Eventbus-Service, mit dem Sie Ihre Anwendungen ganz einfach mit Daten aus einer Vielzahl von Quellen verbinden können. EventBridge liefert einen Stream von Echtzeitdaten aus Ihren eigenen Anwendungen, Software-as-a-Service (SaaS-) Anwendungen und Amazon-Diensten und leitet diese Daten an Ziele wie Lambda weiter. Auf diese Weise können

Sie Ereignisse überwachen, die in Services auftreten, und ereignisgesteuerte Architekturen erstellen. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.

GuardDuty veröffentlicht EventBridge Benachrichtigungen auf dem Standard-Event-Bus, sobald ein Scanstatus ermittelt wurde. Sie können in Ihrem Konto EventBridge Regeln einrichten, um Ereignisse an andere in Amazon integrierte Dienste zu senden EventBridge. Es gelten die EventBridge Standardpreise. Weitere Informationen finden Sie unter EventBridge Amazon-Preise.

Viele der unten aufgeführten Werte sind Platzhalter für das Beispiel und variieren je nach Scan.

Ergebnisse des Malware-Scans: Ereignisse

Mögliche Detailwerte für Backup:

- „Ergebnis des EBS-Snapshot-Scans zum Schutz vor GuardDuty Schadsoftware“
- „Ergebnis des EC2-AMI-Scans für den GuardDuty Malware-Schutz“
- „Ergebnis des S3-Wiederherstellungspunkt-Scans von GuardDuty Malware Protection“
- „Ergebnis der EBS-Wiederherstellungspunktsuche für GuardDuty Schadsoftware Protection“
- „Ergebnis des EC2-Wiederherstellungspunkt-Scans von GuardDuty Malware Protection“

Beispiel für ein Ereignismuster:

```
{
      "detail-type": ["GuardDuty Malware Protection EC2 AMI Scan Result"],
      "source": ["aws.guardduty"]
}
```

Beispiel für ein Benachrichtigungsschema für einen EC2-AMI-Scan ohne gefundene Bedrohungen:

```
{
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "detail-type": "GuardDuty Malware Protection EC2 AMI Scan Result",
    "source": "aws.guardduty",
    "account": "1111222233334444",
    "time": "2025-11-01T00:00:00Z",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1:1111222233334444:image/
ami-1234567890abcdef0"],
    "detail": {
```

```
        "schemaVersion": "1.0",
        "scanStatus": "COMPLETED",
        "resourceType": "EC2_AMI",
        "scanId": "d41d8cd98f00b204e9800998ecf8427e",
        "scanStatusReason": null,
        "scanType": "ON_DEMAND",
        "triggerType": "GUARDDUTY",
        "scanCategory": "FULL_SCAN",
        "scanStartTime": 1234567890123,
        "scanCompleteTime": 2345678901234,
        "scanResultDetails": {
            "scanResultStatus": "NO_THREATS_FOUND",
            "uniqueThreatCount": null
        }
    }
}
```

Beispiel für ein Benachrichtigungsschema für einen EC2-AMI-Scan mit gefundenen Bedrohungen:

```
{
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "detail-type": "GuardDuty Malware Protection EC2 AMI Scan Result",
    "source": "aws.guardduty",
    "account": "1111222233334444",
    "time": "2025-11-01T00:00:00Z",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1:1111222233334444:image/
ami-1234567890abcdef0"],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "COMPLETED",
        "resourceType": "EC2_AMI",
        "scanId": "d41d8cd98f00b204e9800998ecf8427e",
        "scanStatusReason": null,
        "scanType": "ON_DEMAND",
        "triggerType": "GUARDDUTY",
        "scanCategory": "FULL_SCAN",
        "scanStartTime": 1234567890123,
        "scanCompleteTime": 2345678901234,
        "scanResultDetails": {
            "scanResultStatus": "THREATS_FOUND",
            "uniqueThreatCount": 1,
```

```
            "threats": {
                "name": "EICAR-Test-File (not a virus)",
                "source": "AMAZON",
                "count": 2,
                "itemDetails": [{
                    "resourceArn": "arn:aws:ec2:us-east-1:1111222233334444:snapshot/
snap-abcdef01234567890",
                    "hash":
 "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855",
                    "itemPath": "/eicar.txt",
                    "additionalInfo": {
                        "versionId": null,
                        "deviceName": "/dev/sdf"
                    }
                }]
            }
        }
    }
}
```

Beispiel für ein Benachrichtigungsschema für einen übersprungenen EC2-AMI-Scan:

```
{
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
    "detail-type": "GuardDuty Malware Protection EC2 AMI Scan Result",
    "source": "aws.guardduty",
    "account": "1111222233334444",
    "time": "2025-11-01T00:00:00Z",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1:1111222233334444:image/
ami-1234567890abcdef0"],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "SKIPPED",
        "resourceType": "EC2_AMI",
        "scanId": "d41d8cd98f00b204e9800998ecf8427e",
        "scanStatusReason": "UNSUPPORTED_AMI",
        "scanType": "ON_DEMAND",
        "triggerType": "GUARDDUTY",
        "scanCategory": "FULL_SCAN",
        "scanStartTime": 1234567890123,
        "scanCompleteTime": 2345678901234,
```

```
        "scanResultDetails": {
             "uniqueThreatCount": null,
             "threats": null
         }
    }
}
```

Kontingente für den Schutz vor Schadsoftware für Backups

Malware-Schutz für Backup-Kontingente

Kontingentname	AWS Standard-Kontingentwert	Ist er einstellbar?	Description
StartMalwareScan TPS-Limit für alle Ressourcentypen	10	Nein	
Maximale Snapshot-Größe wird unterstützt	2 TB	Nein	
Unterstützte Dateisysteme für Snapshot- und AMI-Scans	• Dateisystem mit neuer Technologie (NTFS) • X-Dateisystem (XFS) • Zweites erweitertes Dateisystem (ext2) • Viertes erweitertes Dateisystem (ext4) • Dateisystem mit Dateizuor	Nein	

Kontingentname	AWS Standard-Kontingentwert	Ist er einstellbar?	Description
	dnungstabelle (FAT) • Virtuelles Dateisystem mit Dateizuordnungstabelle (VFAT)		
Maximale Anzahl von Snapshots innerhalb eines AMI, die für Malware-Scans unterstützt werden	40 für einen vollständigen Scan. Wenn es mehr als 40 sind, GuardDuty werden nur 40 von allen Schnappschüssen gescannt. Bei einem inkrementellen Scan wird das Scannen übersprungen.	Nein	

Kontingentname	AWS Standard-Kontingentwert	Ist er einstellbar?	Description
Maximale Größe eines Objekts innerhalb eines S3-Wiederherstellungspunkts	100 GB	Nein	Die maximale S3-Objektgröße, mit der versucht GuardDuty wird, nach Malware zu suchen. Dieses Kontingent ist zwar nicht anpassbar, aber wenn Sie größere Objekte scannen müssen, wenden Sie sich an den Support, um zu ermitteln, ob das Kontingent für Ihren Anwendungsfall erhöht werden GuardDuty kann.
Extrahierte Archivbytes	100 GB	Nein	Die maximale Datenmenge, die aus einer Archivdatei extrahiert und analysiert werden GuardDuty kann. GuardDuty überspringt das Extrahieren von Archivdateien auf mehr als 100 GB.

Kontingentname	AWS Standard-Kontingentwert	Ist er einstellbar?	Description
Extrahierte Archivdateien	10.000	Nein	Die maximale Anzahl von Dateien, die in einer Archivdatei extrahiert und analysiert werden GuardDuty können. Wenn das Archiv mehr als 10.000 Dateien enthält, muss die archivierte Datei übersprungen GuardDuty werden. **Note** Zusammengesetzte Dateitypen unterliegen möglicherweise diesen Beschränkungen. Zu den Dateitypen gehören MIME-kodierte E-Mail-Nachrichten (Multipurpose Internet Mail Extensions), kompilierte Python-Dateien (PYC), kompilierte HTML-Hilfedateien (CHM), alle Installationsprogramme und ODF-Dokumente (OpenDocument Format).
Maximale Archivtiefe	5	Nein	Die maximale Anzahl verschachtelter Archive, die extrahiert GuardDuty werden können. Wenn das Archiv Dateien enthält, die über diesen Wert hinaus verschachtelt sind, GuardDuty werden diese verschachtelten Dateien übersprungen.

GuardDuty RDS-Schutz

> **Note**
>
> Sie können RDS Protection zusammen mit allen anderen Schutzplänen von einer einzigen Seite in der GuardDuty Konsole aus konfigurieren. Weitere Informationen finden Sie unter Schutzpläne konfigurieren.

RDS Protection in Amazon GuardDuty analysiert und profiliert die RDS-Anmeldeaktivitäten im Hinblick auf potenzielle Zugriffsbedrohungen auf Ihre Amazon Aurora-Datenbanken (Amazon Aurora MySQL-Compatible Edition und Aurora PostgreSQL-Compatible Edition) und Amazon RDS for PostgreSQL.

RDS Protection hilft Ihnen dabei, potenziell verdächtiges Anmeldeverhalten in diesen unterstützten Datenbanken zu identifizieren. GuardDuty Überwacht und protokolliert RDS-Anmeldeaktivität kontinuierlich anomale Aktivitäten. Beispielsweise hat ein zuvor unsichtbarer externer Akteur unbefugten Zugriff auf Ihre Datenbank, oder ein Gegner versucht, Brute-Force-Zugriff zu erhalten, indem er das Passwort der Datenbank errät.

Mit der Einführung von Amazon Aurora PostgreSQL Limitless Database GuardDuty erweitert RDS Protection jetzt auch die Überwachung der Anmeldeaktivitäten von Limitless Databases aus. Alle AWS-Konten , die RDS Protection bereits aktiviert haben, GuardDuty werden automatisch mit der Überwachung der Anmeldedaten aus ihren Limitless-Datenbanken beginnen. Für Konten, die den RDS-Schutz noch nicht aktiviert haben, können Sie mehr über den erfahren 30-day free trial und diese Funktion aktivieren. Informationen zur Aktivierung dieser Funktion finden Sie unter Aktivierung von RDS Protection in Umgebungen mit mehreren Konten oderRDS Protection für ein eigenständiges Konto aktivieren.

> **Hinweis**
>
> Für Read Replica-Instances von RDS for PostgreSQL muss die primäre Datenbankinstanz eine unterstützte Datenbankversion verwenden und erfolgreich aus der Primärdatenbank repliziert werden. Informationen zu Read Replicas finden Sie unter Working with DB Instance Read Replicas im Amazon RDS-Benutzerhandbuch.

RDS Protection erfordert keine zusätzliche Infrastruktur und ist so konzipiert, dass die Leistung Ihrer Datenbank-Instances nicht beeinträchtigt wird. Wenn RDS Protection einen potenziell verdächtigen oder anomalen Anmeldeversuch entdeckt, GuardDuty generiert es einen oder mehrere Erkenntnistypen für RDS Protection mit Details über die potenziell gefährdete Datenbank.

Kostenlose 30-Tage-Testversion

- Wenn Sie die App GuardDuty AWS-Konto in einer neuen Region zum ersten Mal aktivieren, erhalten Sie eine kostenlose 30-Tage-Testversion. In diesem Fall GuardDuty wird auch RDS Protection aktiviert, das in der kostenlosen Testversion enthalten ist. RDS Protection beginnt mit der Überwachung des Anmeldeverhaltens Ihrer Datenbank.
- Wenn Sie RDS Protection bereits verwenden GuardDuty und sich dazu entschließen, RDS Protection in einer neuen Region zum ersten Mal zu aktivieren, erhalten Sie für Ihr Konto in dieser Region eine kostenlose 30-Tage-Testversion von RDS Protection.
- Wenn Sie den RDS-Schutz bereits aktiviert haben, beginnt mit dem Start von Amazon Aurora PostgreSQL Limitless Database GuardDuty automatisch die Überwachung der Anmeldeaktivitäten für die Limitless Databases. Wenn Ihre kostenlose 30-Tage-Testversion von RDS Protection bereits abgelaufen ist, entstehen Ihnen im Zusammenhang mit der Überwachung von Limitless Databases Nutzungskosten.
- Sie können den RDS-Schutz in jeder Region jederzeit deaktivieren.
- Während der kostenlosen 30-Tage-Testversion können Sie eine Schätzung Ihrer Nutzungskosten für dieses Konto und diese Region erhalten. Nach Ablauf der 30-tägigen kostenlosen Testversion wird RDS Protection nicht automatisch deaktiviert. Für Ihr Konto in dieser Region fallen ab sofort Nutzungskosten an. Weitere Informationen finden Sie unter Überwachung der GuardDuty Nutzung und Schätzung der Kosten.

Wenn die RDS-Schutzfunktion nicht aktiviert ist, erkennt GuardDuty es kein anomales oder verdächtiges Anmeldeverhalten. Wenn Sie den RDS-Schutz deaktivieren, stoppt GuardDuty sofort die Überwachung der RDS-Anmeldeaktivitäten und erkennt keine potenzielle Bedrohung für Ihre unterstützten Datenbank-Instances und generiert auch keine zugehörigen Suchtypen.

Informationen darüber AWS-Regionen , wo Aurora PostgreSQL Limitless-Datenbanken unterstützt werden, finden Sie unter Anforderungen für Aurora PostgreSQL Limitless Database.

Unterstützte Amazon Aurora-, Amazon RDS- und Aurora Limitless-Datenbanken

Die folgende Tabelle zeigt die unterstützten Aurora- und Amazon RDS-Datenbankversionen für RDS Protection.

Amazon Aurora und Amazon RDS DB-Engine	Unterstützte Engine-Versionen
Aurora MySQL	• 2.10.2 oder höher • 3.02.1 oder höher • Nachfolgende Hauptversionen
Aurora PostgreSQL	• 10.23 oder höher • 11.12 oder höher • 12.7 oder höher • 13.3 oder höher • 14.3 oder höher • 15.2 oder später • 16.1 oder später • Nachfolgende Hauptversionen
RDS für PostgreSQL	• 11.17 oder später • 12.12 oder später • 13.8 oder später • 14.5 oder später • RDS für PostgreSQL Version 15 • RDS für PostgreSQL Version 16 • RDS für PostgreSQL Version 17 • RDS für PostgreSQL Version 18 • Nachfolgende Hauptversionen
Amazon Aurora PostgreSQL Unbegrenzte Datenbank	• `16.4-limitless` • Nachfolgende Hauptversionen

Amazon Aurora und Amazon RDS DB-Engine	Unterstützte Engine-Versionen
Amazon RDS für MariaDB	• 10.6.25 oder höher • 10.11.16 oder später • 11.4.10 oder später • 11.8.6 oder später • Nachfolgende Hauptversionen
Amazon RDS für MySQL	• 8.0.45 oder höher • 8.4.8 oder später • Nachfolgende Hauptversionen

RDS-Anmeldeaktivität

Wenn Sie die RDS-Schutzfunktion aktivieren, beginnt GuardDuty automatisch die Überwachung der RDS-Anmeldeaktivitäten für Ihre Datenbanken, direkt von den Aurora- und Amazon RDS-Diensten aus. Die RDS-Anmeldeaktivität erfasst sowohl erfolgreiche als auch fehlgeschlagene Anmeldeversuche Unterstützte Amazon Aurora-, Amazon RDS- und Aurora Limitless-Datenbanken in Ihrer AWS Umgebung. Wenn es Hinweise auf ein anomales Anmeldeverhalten gibt, GuardDuty generiert es einen Befund mit Details über die potenziell gefährdete Datenbank. Wenn Sie RDS Protection zum ersten Mal aktivieren oder wenn Sie eine neu erstellte Datenbank-Instance haben, gibt es eine Eingewöhnungszeit, in der Sie die Grundlagen für normales Verhalten festlegen können. Aus diesem Grund kann es vorkommen, dass bei neu aktivierten oder neu erstellten Datenbank-Instances bis zu zwei Wochen lang keine anomale Anmeldung festgestellt wird.

Wenn RDS Protection eine potenzielle Bedrohung erkennt, z. B. ein ungewöhnliches Muster in einer Reihe erfolgreicher, fehlgeschlagener oder unvollständiger Anmeldeversuche, GuardDuty generiert dies einen oder mehrere. Erkenntnistypen für RDS Protection Je nach Art des Befundes kann es Details über das anomale Verhalten enthalten, wie z. B. Anomalien aufgrund von RDS-Anmeldeaktivitäten

GuardDuty verwaltet Unterstützte Datenbanken weder Ihre noch die RDS-Anmeldeaktivitäten und stellt Ihnen auch keine RDS-Anmeldeaktivitäten zur Verfügung.

Aktivierung von RDS Protection in Umgebungen mit mehreren Konten

In einer Umgebung mit mehreren Konten hat nur das delegierte GuardDuty Administratorkonto die Möglichkeit, die RDS-Schutzfunktion für die Mitgliedskonten in ihrer Organisation zu aktivieren oder zu deaktivieren. Die GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Das delegierte GuardDuty Administratorkonto verwaltet ihre Mitgliedskonten mithilfe von AWS Organizations. Dieses delegierte GuardDuty Administratorkonto kann die automatische Überwachung der RDS-Anmeldeaktivitäten für alle neuen Konten aktivieren, wenn diese der Organisation beitreten. Weitere Informationen zu Umgebungen mit mehreren Konten finden Sie unter. Mehrere Konten in GuardDuty

RDS-Schutz für ein delegiertes Administratorkonto aktivieren GuardDuty

Wählen Sie Ihre bevorzugte Zugriffsmethode, um RDS Login Activity Monitoring für das delegierte GuardDuty Administratorkonto zu konfigurieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/
2. Wählen Sie im Navigationsbereich Protection Plans aus.
3. Wählen Sie Alle Aktivierungen konfigurieren aus.
4. Führen Sie eine der folgenden Aktionen aus:

   Verwenden Für alle Konten aktivieren

   - Wählen Sie Für alle Konten aktivieren. Dadurch wird der Schutzplan für alle aktiven GuardDuty Konten in Ihrer AWS Organisation aktiviert, einschließlich der neuen Konten, die der Organisation beitreten.
   - Wählen Sie Speichern.

   Verwenden Konten manuell konfigurieren

   - Um den Schutzplan nur für das Konto des delegierten GuardDuty Administratorkontos zu aktivieren, wählen Sie Konten manuell konfigurieren.
   - Wählen Sie im Abschnitt Konto für delegierte GuardDuty Administratoren (dieses Konto) die Option Aktivieren aus.

- Wählen Sie Speichern.

API/CLI

Führen Sie den updateDetector API-Vorgang mit Ihrer eigenen regionalen Detektor-ID aus und übergeben Sie das `features` Objekt `name` als `RDS_LOGIN_EVENTS` und `status` als`ENABLED`.

Alternativ können Sie es verwenden, AWS CLI um den RDS-Schutz zu aktivieren. Führen Sie den folgenden Befehl aus und *`12abc34d567e8fa901bc2d34e56789f0`* ersetzen Sie ihn durch die Detektor-ID Ihres Kontos und *`us-east-1`* durch die Region, in der Sie den RDS-Schutz aktivieren möchten.

Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
region us-east-1 --features '[{"Name": "RDS_LOGIN_EVENTS", "Status": "ENABLED"}]'
```

Auto-enable RDS-Schutz für alle Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um das Feature RDS Protection für alle Mitgliedskonten zu aktivieren. Dazu gehören der delegierte Administrator, bestehende Mitgliedskonten und die neuen Konten, die der Organisation beitreten.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Stellen Sie sicher, dass Sie die Anmeldedaten für das delegierte GuardDuty Administratorkonto verwenden.

2. Führen Sie eine der folgenden Aktionen aus:

   Verwendung der Schutzpläne angezeigten

   1. Wählen Sie im Navigationsbereich die Option Protection Plans aus.
   2. Wählen Sie Alle Aktivierungen konfigurieren aus.

3. Wählen Sie unter RDS-Schutz die Option Für alle Konten aktivieren aus. Diese Aktion aktiviert automatisch RDS Protection sowohl für bestehende als auch für neue Konten in der Organisation.
4. Wählen Sie „Alle speichern“ und dann „Bestätigen und speichern“.

> **Note**
>
> Die Aktualisierung der Konfiguration der Mitgliedskonten kann bis zu 24 Stunden dauern.

Verwendung der Konten angezeigten

1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
2. Wähle auf der Seite „Konten“ die Option Auto-enable „Einstellungen“ vor „Konten per Einladung hinzufügen“ aus.
3. Wählen Sie im Fenster Einstellungen für automatische Aktivierung verwalten unter RDS Login Activity Monitoring die Option Für alle Konten aktivieren.
4. Wählen Sie Speichern.

Falls Sie die Option Für alle Konten aktivieren nicht verwenden können, finden Sie weitere Informationen unter Aktivieren Sie RDS Protection selektiv für Mitgliedskonten.

API/CLI

Um den RDS-Schutz für Ihre Mitgliedskonten wahlweise zu aktivieren oder zu deaktivieren, rufen Sie den updateMemberDetectors API-Vorgang mit Ihrem eigenen auf. *`detector ID`*

Alternativ können Sie es verwenden, um den AWS CLI RDS-Schutz zu aktivieren. Führen Sie den folgenden Befehl aus und *`12abc34d567e8fa901bc2d34e56789f0`* ersetzen Sie ihn durch die Detektor-ID Ihres Kontos und *`us-east-1`* durch die Region, in der Sie den RDS-Schutz aktivieren möchten.

Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --region us-east-1 --account-ids 111122223333 --features '[{"name":
 "RDS_LOGIN_EVENTS", "status": "ENABLED"}]'
```

Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

RDS Protection für alle vorhandenen aktiven Mitgliedskonten aktivieren

Wählen Sie Ihre bevorzugte Zugriffsmethode, um RDS Protection für alle vorhandenen aktiven Mitgliedskonten in Ihrer Organisation zu aktivieren. Die Mitgliedskonten, die bereits GuardDuty aktiviert wurden, werden als bestehende aktive Mitglieder bezeichnet.

Console

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Melden Sie sich mit den Anmeldedaten für das delegierte GuardDuty Administratorkonto an.
2. Wählen Sie im Navigationsbereich Protection Plans aus.
3. Wählen Sie Alle Aktivierungen konfigurieren aus. Unter RDS Protection können Sie den aktuellen Status der Konfiguration einsehen. Wählen Sie im Abschnitt Aktive Mitgliedskonten die Option Aktionen.
4. Wählen Sie im Dropdownmenü Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten.
5. Wählen Sie Bestätigen aus.

API/CLI

Führen Sie den updateMemberDetectors API-Vorgang mit Ihrem eigenen aus*detector ID*.

Alternativ können Sie es verwenden, AWS CLI um den RDS-Schutz zu aktivieren. Führen Sie den folgenden Befehl aus und *12abc34d567e8fa901bc2d34e56789f0* ersetzen Sie ihn durch

die Detektor-ID Ihres Kontos und *us-east-1* durch die Region, in der Sie den RDS-Schutz aktivieren möchten.

Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --region us-east-1 --account-ids 111122223333 --features '[{"name":
 "RDS_LOGIN_EVENTS", "status": "ENABLED"}]'
```

Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Auto-enable RDS Protection für neue Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um RDS Protection für neue Konten, die Ihrer Organisation beitreten, zu aktivieren.

Console

Das delegierte GuardDuty Administratorkonto kann über die Konsole für neue Mitgliedskonten in einer Organisation aktiviert werden. Verwenden Sie dazu entweder die Seite RDS Protection oder Accounts.

So aktivieren Sie RDS Protection für neue Mitgliedskonten automatisch

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

   Stellen Sie sicher, dass Sie die Anmeldedaten für das delegierte GuardDuty Administratorkonto verwenden.
2. Führen Sie eine der folgenden Aktionen aus:
   - Verwenden Sie die Seite „Schutzpläne“:

     1. Wählen Sie im Navigationsbereich die Option Schutzpläne aus.

2. Wählen Sie Alle Aktivierungen konfigurieren aus.
3. Wählen Sie Konten manuell konfigurieren.
4. Wählen Sie Automatisch für neue Mitgliedskonten aktivieren. Dieser Schritt stellt sicher, dass bei jedem Beitritt eines neuen Kontos zu Ihrer Organisation RDS Protection automatisch für das Konto aktiviert wird. Nur das delegierte GuardDuty Administratorkonto der Organisation kann diese Konfiguration ändern.
5. Wählen Sie Speichern.

- Verwenden der Seite Konten:

1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
2. Wählen Sie auf der Seite Konten die Auto-enable Einstellungen aus.
3. Wählen Sie im Fenster Einstellungen für automatische Aktivierung verwalten unter RDS Login Activity Monitoring die Option Für neue Konten aktivieren.
4. Wählen Sie Speichern.

API/CLI

Um den RDS-Schutz für Ihre Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren, rufen Sie den UpdateOrganizationConfiguration API-Vorgang mit Ihrem eigenen auf. *detector ID*

Alternativ können Sie es verwenden, um den AWS CLI RDS-Schutz zu aktivieren. Führen Sie den folgenden Befehl aus und *12abc34d567e8fa901bc2d34e56789f0* ersetzen Sie ihn durch die Detektor-ID Ihres Kontos und *us-east-1* durch die Region, in der Sie den RDS-Schutz aktivieren möchten. Wenn Sie es nicht für alle neuen Konten aktivieren möchten, die der Organisation beitreten, legen Sie die Einstellung `autoEnable` auf `NONE` fest.

Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1 --auto-enable --features
 '[{"Name": "RDS_LOGIN_EVENTS", "AutoEnable": "NEW"}]'
```

Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto

Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Aktivieren Sie RDS Protection selektiv für Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um die Überwachung der RDS-Anmeldeaktivitäten für Mitgliedskonten selektiv zu aktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

   Stellen Sie sicher, dass Sie die Anmeldedaten für das delegierte GuardDuty Administratorkonto verwenden.
2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.

   Auf der Seite Konten finden Sie in der Spalte RDS-Anmeldeaktivität den Status Ihres Mitgliedskontos.
3. So können Sie die RDS-Anmeldeaktivität selektiv aktivieren oder deaktivieren

   Wählen Sie das Konto aus, für das Sie RDS Protection konfigurieren möchten. Sie können mehrere Konten gleichzeitig auswählen. Wählen Sie im Dropdown-Menü Schutzpläne bearbeiten die Option RDS-Anmeldeaktivität und dann die entsprechende Option aus.

API/CLI

Um den RDS-Schutz für Ihre Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren, rufen Sie den updateMemberDetectors API-Vorgang mit Ihrem eigenen auf. *`detector ID`*

Alternativ können Sie es verwenden, um den AWS CLI RDS-Schutz zu aktivieren. Führen Sie den folgenden Befehl aus und *`12abc34d567e8fa901bc2d34e56789f0`* ersetzen Sie ihn durch die Detektor-ID Ihres Kontos und *`us-east-1`* durch die Region, in der Sie den RDS-Schutz aktivieren möchten.

Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --region us-east-1 --account-ids 111122223333 --features '[{"Name":
 "RDS_LOGIN_EVENTS", "Status": "ENABLED"}]'
```

> **Note**
>
> Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

RDS Protection für ein eigenständiges Konto aktivieren

Ein eigenständiges Konto besitzt die Entscheidung, ob ein Schutzplan AWS-Konto in einem bestimmten Bereich aktiviert oder deaktiviert werden soll AWS-Region.

Wenn Ihr Konto durch oder durch AWS Organizations die Einladungsmethode mit einem GuardDuty Administratorkonto verknüpft ist, gilt dieser Abschnitt nicht für Ihr Konto. Weitere Informationen finden Sie unter Aktivierung von RDS Protection in Umgebungen mit mehreren Konten.

Nachdem Sie RDS Protection aktiviert haben, GuardDuty beginnt RDS-Anmeldeaktivität die Überwachung der unterstützten Datenbanken in Ihrem Konto.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um RDS Protection für ein eigenständiges Konto zu konfigurieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Protection Plans aus.
3. Wählen Sie Alle Aktivierungen konfigurieren aus. Wählen Sie unter RDS-Schutz die Option Aktivieren aus, um den RDS-Schutz zu aktivieren.
4. Wählen Sie „Alle speichern“ und dann „Bestätigen und speichern“.

API/CLI

Führen Sie den updateDetector API-Vorgang mit Ihrer eigenen regionalen Detektor-ID aus und übergeben Sie das `features` Objekt `name` als `RDS_LOGIN_EVENTS` und `status` als`ENABLED`.

Alternativ können Sie es verwenden, AWS CLI um den RDS-Schutz zu aktivieren. Führen Sie den folgenden Befehl aus und *`12abc34d567e8fa901bc2d34e56789f0`* ersetzen Sie ihn durch die Detektor-ID Ihres Kontos und *`us-east-1`* durch die Region, in der Sie den RDS-Schutz aktivieren möchten.

Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
region us-east-1 --features '[{"Name" : "RDS_LOGIN_EVENTS", "Status" : "ENABLED"}]'
```

Behebung von Problemen bei der Überwachung von RDS Protection

GuardDuty RDS Protection analysiert und profiliert Ihre RDS-Anmeldeaktivitäten im Hinblick auf potenzielle Zugriffsbedrohungen für dieUnterstützte Datenbanken. Um Sicherheitstelemetrie effektiv erfassen zu können, GuardDuty muss Ihre Datenbank konfiguriert sein und problemlos funktionieren. Wenn Ihre Datenbank falsch konfiguriert ist oder Probleme auftreten, kann dies die Sicherheitsüberwachung beeinträchtigen.

Der folgende Abschnitt enthält häufig auftretende Probleme und Schritte zu deren Behebung.

RDS-Speicher voll

Wenn Ihrer RDS-Instance der Speicherplatz ausgeht, erfasst sie GuardDuty möglicherweise keine Sicherheitstelemetrie. Das Erreichen der DB-Instance-Speicherkapazitätszuweisung (`storage-full`) ist ein kritischer Status, und RDS empfiehlt, dieses Problem sofort zu beheben. Weitere Informationen finden Sie unter Instance-Status anzeigen im Amazon RDS-Benutzerhandbuch.

Um den `storage-full` Status zu beheben, können Sie eine der folgenden Aktionen ausführen:

- Automatische Speicherskalierung aktivieren (empfohlen) — Aktivieren Sie Amazon RDS-Speicher-Autoscaling, um die Speicherkapazität automatisch zu verwalten und zukünftige `storage-full`

Probleme zu vermeiden. Weitere Informationen finden Sie im Amazon RDS-Benutzerhandbuch unter Automatische Kapazitätsverwaltung mit Amazon RDS-Speicher-Autoscaling.

- Überwachen Sie Ihre Speichernutzung — Überprüfen Sie Ihre Speichernutzung mit einer der folgenden Methoden:
  - Verwenden Sie CloudWatch Metriken, um Details zum Speicher anzuzeigen. Weitere Informationen finden Sie unter CloudWatch Database Insights im CloudWatch Amazon-Benutzerhandbuch.
  - Um Speichermetriken anzuzeigen, folgen Sie den Schritten unter Überwachen von Metriken in einer Amazon RDS-Instance im Amazon RDS-Benutzerhandbuch.
- Speicherkapazität ändern — Informationen zur Erhöhung der Speicherkapazität Ihrer Instance finden Sie unter Erhöhung der DB-Instance-Speicherkapazität im Amazon RDS-Benutzerhandbuch.

Nicht unterstützte Versionen der Primärdatenbank für RDS for PostgreSQL

Für Read Replica-Instances von RDS for PostgreSQL muss die primäre Datenbankinstanz eine unterstützte Datenbankversion haben und erfolgreich aus der Primärdatenbank repliziert werden. GuardDuty überwacht Ihre Instances nur, wenn diese Anforderungen erfüllt sind.

Gehen Sie wie folgt vor, um das Problem mit der nicht unterstützten Version zu beheben:

- Überprüfen Sie die Kompatibilität der Datenbankversionen — Stellen Sie sicher, dass auf Ihrer primären RDS for PostgreSQL-Datenbank eine der unterstützten Versionen ausgeführt wird. Weitere Informationen finden Sie unter Unterstützte Datenbanken.
- Behebung potenzieller Replikationsprobleme — Prüfen und beheben Sie alle Replikationsprobleme zwischen Primär- und Replikat-Instances. Weitere Informationen dazu finden Sie unter Working with read replicas for RDS for PostgreSQL im Amazon RDS-Benutzerhandbuch.

Zusätzliche Sicherheitsüberlegungen

Wenn Ihr Unternehmen strenge Compliance-Anforderungen hat, empfehlen wir, zusätzlich zur Verwendung von RDS Protection eine Datenbanküberprüfung durchzuführen. Weitere Informationen zu Ihren Sicherheitsaufgaben und Ihrem Modell der geteilten Verantwortung finden Sie unter Sicherheit in Amazon RDS im Amazon RDS-Benutzerhandbuch.

GuardDuty Lambda-Schutz

> **Note**
>
> Sie können Lambda Protection zusammen mit allen anderen Schutzplänen von einer einzigen Seite in der GuardDuty Konsole aus konfigurieren. Weitere Informationen finden Sie unter Schutzpläne konfigurieren.

Lambda Protection hilft Ihnen dabei, potenzielle Sicherheitsbedrohungen zu identifizieren, wenn eine AWS Lambda-Funktion in Ihrer AWS -Umgebung aufgerufen wird. Wenn Sie Lambda Protection aktivieren, GuardDuty beginnt die Überwachung der Lambda-Netzwerkaktivitätsprotokolle. Dazu gehören VPC Flow Logs alle Lambda-Funktionen für Ihr Konto (einschließlich der Protokolle, die kein VPC-Netzwerk verwenden) und Protokolle, die generiert werden, wenn die Lambda-Funktion aufgerufen wird. When GuardDuty identifiziert verdächtigen Netzwerkverkehr, der auf das Vorhandensein eines potenziell schädlichen Codes in Ihrer Lambda-Funktion hinweist, und GuardDuty generiert einen oder mehrere. Lambda-Protection-Erkenntnistypen

Kostenlose 30-Tage-Testversion

In der folgenden Liste wird erklärt, wie die kostenlose 30-Tage-Testversion für Ihr Konto funktioniert:

- Wenn Sie die Aktivierung GuardDuty AWS-Konto in einer neuen Region zum ersten Mal durchführen, erhalten Sie eine kostenlose 30-Tage-Testversion. In diesem Fall GuardDuty wird auch Lambda Protection aktiviert, das in der kostenlosen Testversion enthalten ist.
- Wenn Sie Lambda Protection bereits verwenden GuardDuty und sich entscheiden, es zum ersten Mal zu aktivieren, erhält Ihr Konto in dieser Region eine kostenlose 30-Tage-Testversion für Lambda Protection.
- Sie können Lambda Protection in jeder Region jederzeit deaktivieren.
- Während der kostenlosen 30-Tage-Testversion erhalten Sie eine Schätzung Ihrer Nutzungskosten für dieses Konto und diese Region. Nach Ablauf der kostenlosen 30-Tage-Testversion wird Lambda Protection nicht automatisch deaktiviert. Für Ihr Konto in dieser Region fallen ab sofort Nutzungskosten an. Weitere Informationen finden Sie unter Überwachung der GuardDuty Nutzung und Schätzung der Kosten.

Lambda-Netzwerkaktivitätsprotokolle können sich ändern, einschließlich der Erweiterung auf andere Netzwerkaktivitäten wie DNS-Abfragedaten, die durch den Aufruf der Lambda-Funktionen generiert werden. Die Ausweitung auf andere Formen der Überwachung der Netzwerkaktivität wird das Datenvolumen erhöhen, das für Lambda Protection verarbeitet GuardDuty wird. Dies wird sich direkt auf die Nutzungskosten von Lambda Protection auswirken. Wenn GuardDuty mit der Überwachung eines zusätzlichen Netzwerkaktivitätsprotokolls begonnen wird, erhalten die Konten, die Lambda Protection aktiviert haben, mindestens 30 Tage vor der Veröffentlichung eine Benachrichtigung.

> **Note**
>
> Lambda Network Activity Monitoring beinhaltet keine Protokolle für Lambda@Edge-Funktionen.

Lambda Network Activity Monitoring

Wenn Sie Lambda Protection aktivieren, GuardDuty überwacht Lambda-Netzwerkaktivitätsprotokolle, die generiert werden, wenn eine Ihrem Konto zugeordnete Lambda-Funktion aufgerufen wird. Auf diese Weise können Sie potenzielle Sicherheitsbedrohungen für die Lambda-Funktion erkennen. Für Lambda-Funktionen, die für die Verwendung von VPC-Netzwerken konfiguriert sind, müssen Sie keine VPC-Flussprotokolle für die von Lambda für erstellten Elastic Network Interfaces (ENI) aktivieren. GuardDuty GuardDuty berechnet nur die Menge an Lambda-Netzwerkaktivitätsprotokollen, die verarbeitet wurden (in GB), um ein Ergebnis zu generieren. GuardDuty optimiert die Kosten durch die Anwendung intelligenter Filter und die Analyse einer Teilmenge der Lambda-Netzwerkaktivitätsprotokolle, die für die Bedrohungserkennung relevant sind.

GuardDuty verwaltet Ihre Lambda-Netzwerkaktivitätsprotokolle (einschließlich VPC- und Nicht-VPC-Flow-Logs) nicht und macht sie auch nicht in Ihrem Konto zugänglich.

Lambda-Schutz in Umgebungen mit mehreren Konten aktivieren

In einer Umgebung mit mehreren Konten hat nur das delegierte GuardDuty Administratorkonto die Möglichkeit, Lambda Protection für die Mitgliedskonten in seiner Organisation zu aktivieren oder zu deaktivieren. Die GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Das delegierte GuardDuty Administratorkonto verwaltet Mitgliedskonten mithilfe von AWS Organizations. Das delegierte GuardDuty Administratorkonto kann festlegen, dass Lambda Network Activity Monitoring für alle neuen Konten automatisch aktiviert wird, sobald sie der Organisation

beitreten. Weitere Informationen zu Umgebungen mit mehreren Konten finden Sie unter Verwaltung mehrerer Konten bei Amazon. GuardDuty

Lambda-Schutz für delegiertes Administratorkonto GuardDuty aktivieren

Wählen Sie Ihre bevorzugte Zugriffsmethode, um Lambda Network Activity Monitoring für das delegierte GuardDuty Administratorkonto zu aktivieren oder zu deaktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/
2. Wählen Sie im Navigationsbereich unter Einstellungen die Option Lambda Protection.
3. Wählen Sie auf der Seite Lambda Protection die Option Bearbeiten.
4. Führen Sie eine der folgenden Aktionen aus:

   Verwendung von Für alle Konten aktivieren

   - Wählen Sie Für alle Konten aktivieren. Dadurch wird der Schutzplan für alle aktiven GuardDuty Konten in Ihrer AWS Organisation aktiviert, einschließlich der neuen Konten, die der Organisation beitreten.
   - Wählen Sie Speichern.

   Verwendung von Konten manuell konfigurieren

   - Um den Schutzplan nur für das delegierte GuardDuty Administratorkonto zu aktivieren, wählen Sie Konten manuell konfigurieren.
   - Wählen Sie im Abschnitt für das delegierte GuardDuty Administratorkonto (dieses Konto) die Option Aktivieren aus.
   - Wählen Sie Speichern.

API/CLI

Führen Sie den updateDetectorAPI-Vorgang mit Ihrer eigenen regionalen Detektor-ID aus und übergeben Sie das `features` Objekt `name` als `LAMBDA_NETWORK_LOGS` und `status` als`ENABLED`.

Alternativ können Sie AWS CLI Lambda Protection aktivieren. Führen Sie den folgenden Befehl aus und *12abc34d567e8fa901bc2d34e56789f0* ersetzen Sie ihn durch die Detektor-ID Ihres Kontos und *us-east-1* durch die Region, in der Sie Lambda Protection aktivieren möchten.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
region us-east-1 --features '[{"Name": "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

Auto-enable Überwachung der Lambda-Netzwerkaktivität für alle Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um Lambda Network Activity Monitoring Feature für alle Mitgliedskonten zu aktivieren. Dazu gehören der delegierte Administrator, bestehende Mitgliedskonten und die neuen Konten, die der Organisation beitreten.

Console

1. Melden Sie sich bei an AWS-Managementkonsole und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.

2. Führen Sie eine der folgenden Aktionen aus:

   Verwenden Sie die Seite „Schutzpläne“

   1. Wählen Sie im Navigationsbereich Schutzpläne aus.
   2. Wählen Sie Alle Aktivierungen konfigurieren aus.
   3. Wählen Sie unter Lambda-Schutz die Option Für alle Konten aktivieren aus. Diese Aktion aktiviert automatisch Lambda Network Activity Monitoring sowohl für bestehende als auch für neue Konten in der Organisation.
   4. Wählen Sie Alle speichern und anschließend Bestätigen und speichern.

> **Note**
>
> Die Aktualisierung der Konfiguration der Mitgliedskonten kann bis zu 24 Stunden dauern.

Verwenden der Seite Konten

1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
2. Wählen Sie auf der Account-Seite Auto-enableEinstellungen und dann Accounts auf Einladung hinzufügen aus.
3. Wählen Sie im Fenster Einstellungen für automatische Aktivierung verwalten unter Lambda Network Activity Monitoring die Option Für alle Konten aktivieren.

   > **Note**
   >
   > Standardmäßig aktiviert diese Aktion automatisch die Option Auto-enable GuardDuty für neue Mitgliedskonten.

4. Wählen Sie Speichern.

Falls Sie die Option Für alle Konten aktivieren nicht verwenden können, finden Sie weitere Informationen unter Selektives Aktivieren oder Deaktivieren von Lambda Network Activity Monitoring für Mitgliedskonten.

API/CLI

Um Lambda Network Activity Monitoring für Ihre Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren, rufen Sie den updateMemberDetectorsAPI-Vorgang mit Ihrem eigenen auf. `detector ID`

Alternativ können Sie AWS CLI Lambda Protection aktivieren. Führen Sie den folgenden Befehl aus und `12abc34d567e8fa901bc2d34e56789f0` ersetzen Sie ihn durch die Detektor-ID Ihres Kontos und `us-east-1` durch die Region, in der Sie Lambda Protection aktivieren möchten.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --region us-east-1--features '[{"Name":
 "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Aktivierung von Lambda Network Activity Monitoring für alle vorhandenen aktiven Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um Lambda Network Activity Monitoring für alle vorhandenen aktiven Mitgliedskonten in der Organisation zu aktivieren.

Console

So konfigurieren Sie Lambda Network Activity Monitoring für alle vorhandenen aktiven Mitgliedskonten

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Melden Sie sich mit den Anmeldeinformationen für das delegierte GuardDuty Administratorkonto an.
2. Wählen Sie im Navigationsbereich Schutzpläne aus.
3. Wählen Sie Alle Aktivierungen konfigurieren aus. Unter Lambda Protection können Sie den aktuellen Status der Konfiguration einsehen. Wählen Sie im Abschnitt Aktive Mitgliedskonten die Option Aktionen.
4. Wählen Sie im Dropdownmenü Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten.
5. Wählen Sie Bestätigen aus.

API/CLI

Um Lambda Network Activity Monitoring für Ihre Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren, rufen Sie den updateMemberDetectorsAPI-Vorgang mit Ihrem eigenen auf. *detector ID*

Alternativ können Sie AWS CLI Lambda Protection aktivieren. Führen Sie den folgenden Befehl aus und *12abc34d567e8fa901bc2d34e56789f0* ersetzen Sie ihn durch die Detektor-ID Ihres Kontos und *us-east-1* durch die Region, in der Sie Lambda Protection aktivieren möchten.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --region us-east-1 --account-ids 111122223333 --features '[{"Name":
 "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Auto-enable Lambda Network Activity Monitoring für neue Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um Lambda Network Activity Monitoring für neue Konten, die Ihrer Organisation beitreten, zu aktivieren.

Console

Das delegierte GuardDuty Administratorkonto kann Lambda Network Activity Monitoring für neue Mitgliedskonten in einer Organisation entweder über die Seite Lambda-Schutz oder Konten aktivieren.

Wie Sie die automatische Aktivierung von Lambda Network Activity Monitoring für neue Mitgliedskonten einrichten

1. Öffnen Sie die Konsole unter GuardDuty . https://console.aws.amazon.com/guardduty/

   Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.

2. Führen Sie eine der folgenden Aktionen aus:
   - Verwenden Sie die Seite „Schutzpläne“:
     1. Wählen Sie im Navigationsbereich Schutzpläne aus.
     2. Wählen Sie Alle Aktivierungen konfigurieren aus.
     3. Wählen Sie Konten manuell konfigurieren.
     4. Wählen Sie Automatisch für neue Mitgliedskonten aktivieren. Dieser Schritt stellt sicher, dass Lambda Protection automatisch für das Konto aktiviert wird, wann immer ein neues Konto Ihrer Organisation beitritt. Nur das vom Unternehmen delegierte GuardDuty Administratorkonto kann diese Konfiguration ändern.
     5. Wählen Sie Speichern.
   - Verwenden der Seite Konten:
     1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
     2. Wählen Sie auf der Seite Konten die Option Auto-enableEinstellungen aus.
     3. Wählen Sie im Fenster Einstellungen für automatische Aktivierung verwalten unter Lambda Network Activity Monitoring die Option Für neue Konten aktivieren.
     4. Wählen Sie Speichern.

API/CLI

Um Lambda Network Activity Monitoring für neue Mitgliedskonten zu aktivieren, rufen Sie den UpdateOrganizationConfigurationAPI-Vorgang mit Ihrem eigenen auf. *`detector ID`*

Alternativ können Sie AWS CLI Lambda Protection aktivieren. Das folgende Beispiel zeigt, wie Sie Lambda Network Activity Monitoring für ein einzelnes Mitgliedskonto aktivieren können. *`12abc34d567e8fa901bc2d34e56789f0`*Ersetzen Sie es durch die Detektor-ID Ihres Kontos und *`us-east-1`* durch die Region, in der Sie Lambda Protection aktivieren möchten. Wenn Sie es nicht für alle neuen Konten aktivieren möchten, die der Organisation beitreten, legen Sie die Einstellung `AutoEnable` auf `NONE` fest.

Informationen zur Angabe `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1 --auto-enable --features
 '[{"Name": "LAMBDA_NETWORK_LOGS", "AutoEnable": "NEW"}]'
```

Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Selektives Aktivieren oder Deaktivieren von Lambda Network Activity Monitoring für Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um Lambda Network Activity Monitoring für ausgewählte Mitgliedskonten zu aktivieren oder zu deaktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.
2. Klicken Sie im Navigationsbereich unter Settings auf Accounts.

   Sehen Sie sich auf der Seite Konten die Spalte Lambda Network Activity Monitoring an. Sie gibt an, ob Lambda Network Activity Monitoring aktiviert ist oder nicht.
3. Wählen Sie das Konto aus, für das Sie Lambda Protection konfigurieren möchten. Sie können mehrere Konten gleichzeitig auswählen.
4. Wählen Sie im Dropdownmenü Schutzpläne bearbeiten die Option Lambda Network Activity Monitoring und wählen Sie dann eine entsprechende Aktion aus.

API/CLI

Rufen Sie die updateMemberDetectorsAPI mit Ihrer eigenen auf. *`detector ID`*

Alternativ können Sie AWS CLI Lambda Protection aktivieren. *`12abc34d567e8fa901bc2d34e56789f0`*Ersetzen Sie es durch die Detektor-ID Ihres Kontos und *`us-east-1`* durch die Region, in der Sie Lambda Protection aktivieren möchten.

Informationen zur Angabe `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --region us-east-1 --account-ids 111122223333 --features '[{"Name":
 "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Lambda Protection für ein eigenständiges Konto aktivieren

Ein eigenständiges Konto hat die Entscheidung, einen Schutzplan AWS-Konto in einem bestimmten AWS-Region Bereich zu aktivieren oder zu deaktivieren.

Wenn Ihr Konto über oder über AWS Organizations die Einladungsmethode mit einem GuardDuty Administratorkonto verknüpft ist, gilt dieser Abschnitt nicht für Ihr Konto. Weitere Informationen finden Sie unter Lambda-Schutz in Umgebungen mit mehreren Konten aktivieren.

Nachdem Sie Lambda Protection aktiviert haben, GuardDuty beginnt die Überwachung Lambda Network Activity Monitoring in Ihrem Konto.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um Lambda Protection für ein eigenständiges Konto zu konfigurieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/
2. Wählen Sie im Navigationsbereich unter Einstellungen die Option Lambda Protection.
3. Auf der Lambda-Protection-Seite wird der aktuelle Status Ihres Kontos angezeigt. Wählen Sie Aktivieren, um Lambda Protection in Ihrem Konto zu aktivieren.
4. Wählen Sie Bestätigen, um Ihre Auswahl zu speichern.

API/CLI

Führen Sie den updateDetectorAPI-Vorgang mit Ihrer eigenen regionalen Melder-ID aus und übergeben Sie das `features` Objekt `name` als `LAMBDA_NETWORK_LOGS` und `status` als`ENABLED`.

Alternativ können Sie AWS CLI Lambda Protection aktivieren. Führen Sie den folgenden Befehl aus und *12abc34d567e8fa901bc2d34e56789f0* ersetzen Sie ihn durch die Detektor-ID Ihres Kontos und *us-east-1* durch die Region, in der Sie Lambda Protection aktivieren möchten.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --region us-east-1 --features [{"Name" : "LAMBDA_NETWORK_LOGS", "Status" :
 "ENABLED"}]'
```

GuardDuty Untersuchung (Vorschau)

GuardDuty Die Untersuchung bietet eine AI-powered Sicherheitsanalyse Ihrer GuardDuty Ergebnisse und Konten. Wenn Sie eine Untersuchung erstellen, GuardDuty werden anhand von Wissensdiagrammen der Kontext der Ergebnisse, zugehörige Aktivitäten der letzten 90 Tage, betroffene Ressourcen, Bedrohungsinformationen und Bedrohungsindikatoren untersucht. Jede Untersuchung bietet eine Bewertung der Bedrohungslage mit Vertrauensbewertung, Klassifizierung der MITRE ATT&CK® -Technik, unterstützenden Nachweisen und umsetzbaren Empfehlungen.

Jede Untersuchung liefert die folgenden Erkenntnisse:

- Risikostufe — Eine Bewertung des Gesamtrisikos: Info, Niedrig, Mittel, Hoch oder Kritisch.
- Konfidenz — Das Konfidenzniveau der Bewertung: Unbekannt, Niedrig, Mittel oder Hoch.
- Zusammenfassung — Eine Beschreibung der Untersuchungsergebnisse und der wichtigsten Beobachtungen.
- Einzelheiten der Untersuchung — Zusätzliche Informationen und Kontext im Zusammenhang mit der Untersuchung.
- Empfohlene Maßnahmen — Detaillierte Maßnahmen, einschließlich der CLI-Befehle, können Sie ergreifen, um die identifizierten Probleme zu beheben.

> **Note**
>
> GuardDuty Investigation ist nur in den folgenden 10 AWS Handelsregionen verfügbar: USA Ost (Nord-Virginia), USA Ost (Ohio), USA West (Oregon), Kanada (Zentral), Europa (Frankfurt), Europa (Irland), Europa (London), Europa (Paris), Europa (Stockholm) und Asien-Pazifik (Tokio).

Arten der Analyse

GuardDuty Die Untersuchung unterstützt die folgenden drei Analysearten:

- Ergebnisanalyse — Analysiert spezifische GuardDuty Ergebnisse, wenn Sie die Ergebnis-ID (32 Zeichen hexadezimal) angeben. Als Vorschauversion unterstützt GuardDuty Investigation alle Ergebnisse von Extended Threat Detection (XTD) sowie ausgewählte Ergebnisse aus den Plänen „Fundament“, „S3“ und „Runtime“.

- Kontoanalyse — Analysiert die Bedrohungslage eines AWS Kontos, wenn Sie die 12-stellige AWS Konto-ID angeben.
- Organisationsanalyse — Analysiert die Bedrohungslage Ihres Unternehmens. Als Vorschau werden bis zu 100 Konten analysiert.

Cross-Region Folgerung

GuardDuty Investigation nutzt Cross-Region Inference Service (CRIS), der automatisch das Optimum AWS-Region innerhalb Ihrer Region auswählt, um die Untersuchungsanalyse zu verarbeiten und den Untersuchungsbericht zu erstellen. Dies maximiert die verfügbaren Rechenressourcen und die Modellverfügbarkeit und sorgt für ein optimales Kundenerlebnis.

Ihre Daten bleiben nur in der Region gespeichert, aus der die Ermittlungsanfrage stammt. Ermittlungsdaten und zusammenfassende Ergebnisse können jedoch außerhalb dieser Region verarbeitet werden. Alle Daten werden verschlüsselt über das sichere Netzwerk von Amazon übertragen.

GuardDuty Investigation leitet Ihre Inferenzanfragen sicher an verfügbare Rechenressourcen in dem geografischen Gebiet weiter, aus dem die Anfrage stammt, wie in der folgenden Tabelle dargestellt.

Cross-Region Weiterleitung von Inferenzen

Unterstützte - Regionen	GuardDuty Region	Inferenzregionen
Vereinigte Staaten	USA Ost (Nord-Virginia)	USA Ost (Nord-Virginia), USA Ost (Ohio), USA West (Oregon)
Vereinigte Staaten	USA Ost (Ohio)	USA Ost (Nord-Virginia), USA Ost (Ohio), USA West (Oregon)
Vereinigte Staaten	USA West (Oregon)	USA Ost (Nord-Virginia), USA Ost (Ohio), USA West (Oregon)
Vereinigte Staaten	Kanada (Zentral)	Kanada (Zentral), USA Ost (Nord-Virginia), USA Ost (Ohio), USA West (Oregon)

Unterstützte - Regionen	GuardDuty Region	Inferenzregionen
Europa	Europa (Frankfurt)	Europa (Frankfurt), Europa (Stockholm), Europa (Mailand), Europa (Spanien), Europa (Irland), Europa (Paris)
Europa	Europa (Irland)	Europa (Frankfurt), Europa (Stockholm), Europa (Mailand), Europa (Spanien), Europa (Irland), Europa (Paris)
Europa	Europa (London)	Europa (Frankfurt), Europa (Stockholm), Europa (Mailand), Europa (Spanien), Europa (Irland), Europa (London), Europa (Paris)
Europa	Europa (Paris)	Europa (Frankfurt), Europa (Stockholm), Europa (Mailand), Europa (Spanien), Europa (Irland), Europa (Paris)
Europa	Europa (Stockholm)	Europa (Frankfurt), Europa (Stockholm), Europa (Mailand), Europa (Spanien), Europa (Irland), Europa (Paris)
Japan	Asien-Pazifik (Tokio)	Asien-Pazifik (Tokio), Asien-Pazifik (Osaka)

Voraussetzungen

Bevor Sie GuardDuty Investigation verwenden können, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- In dem Bereich, in AWS-Region dem Sie Untersuchungen durchführen möchten, muss ein aktiver GuardDuty Detektor vorhanden sein. Weitere Hinweise zur Aktivierung finden GuardDuty Sie unterErste Schritte mit GuardDuty.
- Sie müssen die GuardDuty Ermittlungsfunktion auf Ihrem Detektor aktivieren.

  Console

  1. Öffnen Sie die GuardDuty Konsole.

2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie unter KI-gestützte Untersuchungen — Vorschau die Option Aktivieren aus.

API/CLI

Rufen Sie die UpdateDetectorAPI auf und aktivieren Sie die `AI_ANALYST` Funktion auf Ihrem Detektor.

```
aws guardduty update-detector \
    --detector-id 2cb3d4e5f6a7b8c9d0e1f2a3b4c5d6e7 \
    --features '[{"Name": "AI_ANALYST", "Status": "ENABLED"}]'
```

- Ihre IAM-Identität muss über die erforderlichen Berechtigungen verfügen, um Ermittlungsaktionen durchführen zu können. Die folgenden IAM-Aktionen sind erforderlich:
  - `guardduty:CreateInvestigation`— Erforderlich, um eine neue Untersuchung zu erstellen.
  - `guardduty:GetInvestigation`— Erforderlich, um Untersuchungsergebnisse abzurufen.
  - `guardduty:ListInvestigations`— Erforderlich, um Untersuchungen für einen Detektor aufzulisten.

Das folgende Beispiel für eine IAM-Richtlinie gewährt die Erlaubnis, alle GuardDuty Ermittlungsaktionen zu verwenden:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:CreateInvestigation",
                "guardduty:GetInvestigation",
                "guardduty:ListInvestigations"
            ],
            "Resource": "arn:aws:guardduty:us-
west-2:123456789012:detector/2cb3d4e5f6a7b8c9d0e1f2a3b4c5d6e7"
        }
    ]
}
```

Zugriffsmodell für Administrator- und Mitgliedskonten

Je nachdem, ob Sie ein Administratorkonto oder ein Mitgliedskonto verwenden, gelten für GuardDuty Investigation die folgenden Zugriffsregeln:

- Administratorkonten — Sie können Untersuchungen für sich selbst und ihre Mitgliedskonten erstellen, abrufen und auflisten.
- Mitgliedskonten — Sie können nur Untersuchungen für ihr eigenes Konto abrufen und auflisten. Mitgliedskonten können keine Untersuchungen durchführen und nicht auf Untersuchungen zugreifen, die zu anderen Konten oder dem Administratorkonto gehören.

Eine Untersuchung erstellen

Sie können eine Untersuchung erstellen, um GuardDuty Ergebnisse und Konten in Ihrer AWS Umgebung zu analysieren. Die Untersuchung wird asynchron im Hintergrund ausgeführt. Nachdem Sie eine Untersuchung erstellt haben, verwenden Sie die Untersuchungs-ID, um deren Status zu überprüfen und Ergebnisse abzurufen.

> **Important**
>
> Während der Vorschauphase können Sie bis zu 10 Untersuchungen pro Konto und Tag einleiten, mit einem Gesamtlimit von 100 Untersuchungen pro Konto. Fehlgeschlagene Untersuchungen werden nicht auf diese Kontingente angerechnet. Wenn Sie den verwenden API/CLI, kann die Trigger-Eingabeaufforderung bis zu 2.048 Zeichen lang sein.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um eine Untersuchung zu erstellen.

Console

1. Öffnen Sie die GuardDuty Konsole und navigieren Sie im linken Navigationsbereich zu Investigations.
2. Wählen Sie Untersuchung einleiten aus.
3. Wählen Sie einen Untersuchungsbereich aus:
   - Ein bestimmtes Ergebnis — Geben Sie die Ergebnis-ID ein, die Sie analysieren möchten.

- Mein Konto (nur eigenständig) — Keine zusätzlichen Eingaben erforderlich. GuardDuty wird Ihr Konto analysieren.
- Ein bestimmtes Konto (nur Administrator) — Geben Sie die 12-stellige AWS Konto-ID ein.
- Alle Konten in der Organisation (nur Administrator) — Keine zusätzlichen Eingaben erforderlich.

4. Wählen Sie Untersuchung einleiten, um die Analyse zu starten.

API/CLI

Führen Sie den CreateInvestigation API-Vorgang aus, um eine neue Untersuchung zu starten. Sie müssen die Melder-ID und eine Auslöseraufforderung angeben, die beschreibt, was untersucht werden soll.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

```
aws guardduty create-investigation \
    --detector-id 2cb3d4e5f6a7b8c9d0e1f2a3b4c5d6e7 \
    --trigger-prompt "Investigate finding 1ab2c3d4e5f6a7b8c9d0e1f2a3b4c5d6 in
 account 123456789012"
```

Ersetzen Sie im vorherigen Befehl das *`detector-id`* durch Ihre eigene Melder-ID und *`trigger-prompt`* durch eine Beschreibung dessen, was Sie untersuchen möchten.

Sie können optional einen `--client-token` Parameter für Idempotenz angeben. Wenn Sie die Anfrage mit demselben Client-Token erneut versuchen, wird die bestehende Untersuchung GuardDuty zurückgegeben, anstatt ein Duplikat zu erstellen.

Beispielausgabe:

```
{
    "InvestigationId": "a1b2c3d4-5678-90ab-cdef-ef1234567890"
}
```

Anforderungen an die Trigger-Aufforderung

In der Auslöseraufforderung muss beschrieben werden, was untersucht werden soll. GuardDuty bestimmt den Analysetyp anhand des Inhalts Ihrer Eingabeaufforderung:

- Ergebnisanalyse — Geben Sie genau eine Ergebnis-ID (32-stellige hexadezimale Zeichenfolge) in die Eingabeaufforderung ein. Das Ergebnis muss vorhanden sein und zum Konto des Anrufers oder zu einem Mitgliedskonto gehören. Sie können nicht mehrere Such-IDs in einer einzigen Aufforderung angeben.
- Kontoanalyse — Geben Sie genau eine 12-stellige AWS Konto-ID in die Aufforderung ein. Der Anrufer muss der Administrator dieses Kontos sein. Sie können nicht mehrere Konto-IDs in einer einzigen Aufforderung angeben.
- Unternehmensanalyse — Beschreiben Sie in Ihrer Aufforderung ein unternehmensweites Sicherheitsproblem. Die Untersuchung analysiert Signale im gesamten Unternehmen (bis zu 100 Konten).

GuardDuty verwendet KI, um Ihre formlose Aufforderung zu interpretieren und den geeigneten Analyseumfang zu bestimmen. Wenn Sie eine Befund-ID angeben, wird eine Ergebnisanalyse durchgeführt. Wenn Sie eine Konto-ID angeben, wird eine Kontoanalyse durchgeführt. Wenn Ihre Aufforderung ein unternehmensweites Problem beschreibt, wird eine Organisationsanalyse durchgeführt. Wenn die Aufforderung keinem bestimmten Analysetyp entspricht, analysiert die Untersuchung standardmäßig das eigene Konto des Anrufers.

Im Folgenden finden Sie Beispiele für Trigger-Eingabeaufforderungen für jeden Analysetyp:

- Analyse finden — `"Investigate finding 1ab2c3d4e5f6a7b8c9d0e1f2a3b4c5d6 in account 123456789012"`
- Kontoanalyse — `"Analyze findings in account with id 123456789012"`
- Organisationsanalyse — `"Analyze findings in my organization"`

Erstellung einer Untersuchung für ein Mitgliedskonto

Wenn Sie ein Administratorkonto haben, können Sie eine Untersuchung für ein Mitgliedskonto erstellen, indem Sie die Mitgliedskonto-ID in der Auslöseraufforderung angeben. Verwenden Sie die Detektor-ID des Administratorkontos im Befehl. Die Ergebnisse der Untersuchung werden Ergebnisse aus dem angegebenen Mitgliedskonto enthalten.

```
aws guardduty create-investigation \
    --detector-id 2cb3d4e5f6a7b8c9d0e1f2a3b4c5d6e7 \
    --trigger-prompt "Analyze findings in account with id 111122223333"
```

Ersetzen Sie im vorherigen Befehl das *detector-id* durch die Melder-ID Ihres Administratorkontos. Die 12-stellige Konto-ID in der Trigger-Eingabeaufforderung identifiziert das Mitgliedskonto, das untersucht werden soll.

Untersuchungsergebnisse anzeigen

Nachdem Sie eine Untersuchung erstellt haben, können Sie die Ergebnisse einschließlich der Zusammenfassung, der Untersuchungsdetails, des Vertrauensniveaus und der Empfehlung abrufen. Eine Untersuchung kann einen der folgenden Status haben:

- LÄUFT — Die Untersuchung ist noch nicht abgeschlossen.
- ABGESCHLOSSEN — Die Untersuchung wurde erfolgreich abgeschlossen und die Ergebnisse sind verfügbar.
- FEHLGESCHLAGEN — Bei der Untersuchung ist ein Fehler aufgetreten. Einzelheiten finden Sie im Fehlerfeld.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um die Untersuchungsergebnisse einzusehen.

AI-generated Analysen und Empfehlungen können Fehler oder unvollständige Bewertungen enthalten. Eine Überprüfung durch einen Menschen wird empfohlen.

Console

1. Öffnen Sie die GuardDuty Konsole und navigieren Sie im linken Navigationsbereich zu Investigations.
2. Suchen Sie in der Tabelle mit den Untersuchungen nach der abgeschlossenen Untersuchung, die Sie überprüfen möchten.
3. Wählen Sie den Link zum Titel der Untersuchung, um die Detailseite zu öffnen.

> **Note**
>
> Die Titel der Untersuchung können nur angeklickt werden, wenn der Status Abgeschlossen lautet.

API/CLI

Führen Sie den GetInvestigation API-Vorgang aus, um alle Details einer abgeschlossenen Untersuchung abzurufen.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

```
aws guardduty get-investigation \
    --detector-id 2cb3d4e5f6a7b8c9d0e1f2a3b4c5d6e7 \
    --investigation-id a1b2c3d4-5678-90ab-cdef-ef1234567890
```

Beispielausgabe für eine abgeschlossene Untersuchung:

```
{
    "Investigation": {
        "InvestigationId": "a1b2c3d4-5678-90ab-cdef-ef1234567890",
        "Status": "COMPLETED",
        "TriggerPrompt": "Investigate finding 1ab2c3d4e5f6a7b8c9d0e1f2a3b4c5d6 in
 account 123456789012",
        "TriggeredBy": "123456789012",
        "RiskLevel": "Critical",
        "Risk": "Detection logic is valid but no live resources are compromised.",
        "Confidence": "High",
        "Summary": "{\"keyObservations\":{\"title\":\"...\",\"narrative\":\"...\",
\"observations\":[...]},\"countermeasures\":[...],\"threatAssessment\":{...}}",
        "Cloud": {
            "Provider": "AWS",
            "Region": "us-east-1",
            "Account": "123456789012"
        },
        "Metadata": {
            "Product": {
                "Name": "Amazon GuardDuty AI Analyst",
                "Feature": "Investigation"
            },
            "Version": "1.0.0"
        },
        "StartTime": 1705319400.0,
        "EndTime": 1705319700.0
    }
```

```
}
```

Das `Summary` Feld enthält eine JSON-Zeichenfolge mit den vollständigen Untersuchungsergebnissen, einschließlich der wichtigsten Beobachtungen, Gegenmaßnahmen mit CLI-Befehlen und einer MITRE ATT&CK® -Bedrohungsbeurteilung.

Interpretation der Untersuchungsergebnisse

In der folgenden Tabelle werden die Risikoniveaus beschrieben, die sich aus einer Untersuchung ergeben können:

Risikoniveaus einer Untersuchung

Risikoniveau	Description
Info	Informatives Ergebnis ohne festgestelltes Risiko für die Umwelt.
Niedrig	Geringes Risiko, das wahrscheinlich keine sofortigen Maßnahmen erfordert.
Mittel	Moderates Risiko, das Sie überprüfen müssen und das möglicherweise behoben werden muss.
Hoch	Erhebliches Risiko, das umgehend untersucht und behoben werden muss.
Kritisch	Schwerwiegendes Risiko, das sofortige Maßnahmen erfordert, um weitere Kompromisse zu verhindern.

In der folgenden Tabelle werden die Konfidenzniveaus beschrieben:

Konfidenzniveaus für Untersuchungen

Konfidenzniveau	Description
Unbekannt	Unzureichende Daten, um das Vertrauen in die Bewertung zu beurteilen.
Niedrig	Begrenzte Belege stützen die Bewertung.
Mittel	Die Bewertung wird durch mäßige Belege gestützt.

Konfidenzniveau	Description
Hoch	Die Bewertung wird durch stichhaltige Belege gestützt.

Ermittlungen auflisten

Sie können alle Untersuchungen für einen Detektor auflisten, optional mit Sortierung und Seitennummerierung. Auf diese Weise können Sie den Status mehrerer Untersuchungen überprüfen und verfolgen.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um Untersuchungen aufzulisten.

Console

1. Öffnen Sie die GuardDuty Konsole und navigieren Sie im linken Navigationsbereich zu Investigations.
2. In der Tabelle mit den Untersuchungen werden alle Untersuchungen für den aktuellen Detektor mit ihrem Status, ihrer Risikostufe und ihren Zeitstempeln angezeigt.

API/CLI

Führen Sie den ListInvestigations API-Vorgang aus, um die Zusammenfassungen der Untersuchungen für einen Detektor aufzulisten.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

```
aws guardduty list-investigations \
    --detector-id 2cb3d4e5f6a7b8c9d0e1f2a3b4c5d6e7 \
    --max-results 10
```

Sie können die Ergebnisse sortieren, indem Sie einen `--sort-criteria` Parameter angeben. Im folgenden Beispiel sind die Untersuchungen in absteigender Reihenfolge nach Startzeit sortiert:

```
aws guardduty list-investigations \
    --detector-id 2cb3d4e5f6a7b8c9d0e1f2a3b4c5d6e7 \
```

```
    --sort-criteria '{"attributeName": "START_TIME", "orderBy": "DESC"}' \
    --max-results 10
```

Die verfügbaren Sortierattribute sind`START_TIME`,`END_TIME`, `STATUS`RISK_LEVEL, und`CONFIDENCE`. Sie können in `ASC` (aufsteigender) oder `DESC` (absteigender) Reihenfolge sortieren.

Beispielausgabe:

```
{
    "Investigations": [
        {
            "InvestigationId": "a1b2c3d4-5678-90ab-cdef-ef1234567890",
            "Status": "COMPLETED",
            "TriggerPrompt": "Investigate finding 1ab2c3d4e5f6a7b8c9d0e1f2a3b4c5d6
 in account 123456789012",
            "RiskLevel": "Critical",
            "Confidence": "High",
            "StartTime": 1705319400.0,
            "EndTime": 1705319700.0,
            "AccountId": "123456789012"
        },
        {
            "InvestigationId": "b2c3d4e5-6789-01bc-def0-ef2345678901",
            "Status": "COMPLETED",
            "TriggerPrompt": "Analyze findings in account with id 123456789012",
            "RiskLevel": "High",
            "Confidence": "High",
            "StartTime": 1705315800.0,
            "EndTime": 1705316100.0,
            "AccountId": "123456789012"
        },
        {
            "InvestigationId": "c3d4e5f6-7890-12cd-ef01-ef3456789012",
            "Status": "COMPLETED",
            "TriggerPrompt": "Analyze findings in my organization",
            "RiskLevel": "Medium",
            "Confidence": "Medium",
            "StartTime": 1705312200.0,
            "EndTime": 1705312500.0,
            "AccountId": "123456789012"
        }
    ]
```

```
}
```

Wenn die Antwort einen `NextToken` Wert enthält, übergeben Sie ihn in einer nachfolgenden Anfrage, um die nächste Ergebnisseite abzurufen. Sie können bis zu 50 Ergebnisse pro Seite abrufen.

Mehrere Konten bei Amazon GuardDuty

Wenn Ihre AWS Umgebung über mehrere Konten verfügt, können Sie diese verwalten, indem Sie eines AWS-Konto als Administratorkonto festlegen. Anschließend können Sie mehrere Konten AWS-Konten mit diesem Administratorkonto als Mitgliedskonten verknüpfen. Mit dieser Konfiguration kann ein GuardDuty bestimmtes Administratorkonto die Gesamtsicherheit Ihres Unternehmens beurteilen und überwachen. Das Administratorkonto kann auch Aufgaben der Kontoverwaltung ausführen, z. B. die Überprüfung aller generierten Ergebnisse und die Konfiguration der darin enthaltenen Schutzpläne GuardDuty.

GuardDutyIn besteht eine Organisation aus einem delegierten GuardDuty Administratorkonto und einem oder mehreren zugehörigen Mitgliedskonten. Sie können die Konten auf zwei Arten verknüpfen: durch Integration mit AWS Organizations oder durch Verwendung einer herkömmlichen Methode zum Senden und Annehmen von Mitgliedschaftseinladungen in der GuardDuty Konsole. GuardDuty empfiehlt die Integration mit AWS Organizations.

> **Note**
>
> Über die Schaltfläche „Bearbeiten“ im Abschnitt „Automatische Aktivierung“ auf der Seite „Konten“ werden Sie auf die Schutzpläne konfigurieren Seite weitergeleitet, anstatt das alte Konfigurations-Modal zu öffnen.

AWS Organizations ist ein globaler Kontoverwaltungsdienst, der es AWS Administratoren ermöglicht, mehrere AWS-Konten Konten zu konsolidieren und zentral zu verwalten. Er bietet Funktionen zur Kontoverwaltung und konsolidierten Abrechnung, die auf Budget-, Sicherheits- und Compliance-Anforderungen zugeschnitten sind. Es wird ohne zusätzliche Kosten angeboten und lässt sich in mehrere Geräte integrieren AWS-Services, darunter Macie und Amazon GuardDuty. AWS Security Hub CSPM Weitere Informationen finden Sie im AWS Organizations -Benutzerhandbuch.

Inhalt

- Grundlegendes zur Beziehung zwischen GuardDuty Administratorkonto und Mitgliedskonten
- GuardDuty Konten verwalten mit AWS Organizations
- GuardDuty Konten auf Einladung verwalten
- GuardDuty Überlegungen zum Exportieren von Mitgliedskontodaten im CSV-Format

Grundlegendes zur Beziehung zwischen GuardDuty Administratorkonto und Mitgliedskonten

Wenn Sie das Konto GuardDuty in einer Umgebung mit mehreren Konten verwenden, kann das Administratorkonto bestimmte Aspekte von Konten im Namen GuardDuty der Mitgliedskonten verwalten. Ein Administratorkonto kann die folgenden Hauptfunktionen ausführen:

- Zugeordnete Mitgliedskonten hinzufügen und entfernen — Der Vorgang, mit dem ein Administratorkonto dies tun kann, hängt davon ab, wie Sie die Konten verwalten — per AWS Organizations oder nach der GuardDuty Einladungsmethode.

  GuardDuty empfiehlt, Ihre Mitgliedskonten über zu verwalten AWS Organizations.
- Aktivierung des delegierten GuardDuty Administratorkontos GuardDuty im Verwaltungskonto — Falls das AWS Organizations Verwaltungskonto einmal deaktiviert wird GuardDuty, kann das delegierte GuardDuty Administratorkonto GuardDuty im Verwaltungskonto aktiviert werden. Es ist jedoch erforderlich, dass das Verwaltungskonto das nicht ausdrücklich gelöscht hat. Service-linked Rollenberechtigungen für GuardDuty
- Status von Mitgliedskonten konfigurieren — Ein Administratorkonto kann den Status von GuardDuty Schutzplänen aktivieren oder deaktivieren und den Status von im Namen der zugehörigen Mitgliedskonten aktivieren, aussetzen oder deaktivieren. GuardDuty

  Delegierte GuardDuty Administratorkonten, die mit verwaltet werden, AWS Organizations können automatisch aktiviert werden GuardDuty , wenn sie als Mitglieder hinzugefügt AWS-Konten werden.
- Passen Sie an, wann Ergebnisse generiert werden sollen — Ein Administratorkonto kann die Ergebnisse innerhalb des GuardDuty Netzwerks anpassen, indem es Unterdrückungsregeln, Listen vertrauenswürdiger IP-Adressen und Bedrohungslisten erstellt und verwaltet. In einer Umgebung mit mehreren Konten steht die Konfiguration dieser Funktionen nur einem delegierten GuardDuty Administratorkonto zur Verfügung. Ein Mitgliedskonto kann diese Konfiguration nicht aktualisieren.

In der folgenden Tabelle wird die Beziehung zwischen GuardDuty Administratorkonto und Mitgliedskonten detailliert beschrieben.

Schlüssel für die Tabelle

- Selbst — Ein Konto kann die aufgelistete Aktion nur für sein eigenes Konto ausführen.
- Beliebig — Ein Konto kann die aufgelistete Aktion für jedes zugehörige Konto ausführen.

- Alle — Ein Konto kann die aufgelistete Aktion ausführen und sie gilt für alle zugehörigen Konten. In der Regel handelt es sich bei dem Konto, das diese Aktion durchführt, um ein GuardDuty bestimmtes Administratorkonto
- Zellen mit Bindestrich (—) — Tabellenzellen mit Bindestrich (—) geben an, dass das Konto die aufgeführte Aktion nicht ausführen kann.

Action (Aktion)	Durch AWS Organizations		Auf Einladung	
	Delegiertes GuardDuty Administratorkonto	Zugeordnetes Mitgliedskonto	GuardDuty Administratorkonto	Zugeordnetes Mitgliedskonto
Aktiviere GuardDuty	Beliebig	–	Selbst	Selbst
GuardDuty Automatisch für die gesamte Organisation aktivieren (`ALL`,`NEW`,`NONE`)	Alle	–	–	–
Alle Mitgliedskonten der Organisationen unabhängig vom GuardDuty Status anzeigen	Beliebig	–	–	–
Generieren Sie Beispielergebnisse	Selbst	Selbst	Selbst	Selbst
Alle GuardDuty Ergebnisse anzeigen	Beliebig	Selbst	Beliebig	Selbst

GuardDuty Ergebnisse archivieren	Beliebig	–	Beliebig	–
Anwenden von Unterdrückungsregeln	Alle	–	Alle	–
Erstellen Sie eine Liste vertrauenswürdiger IP-Adressen oder Bedrohungslisten	Alle	–	Alle	–
Aktualisieren Sie die Liste der vertrauenswürdigen IP-Adressen oder der Bedrohungslisten	Alle	–	Alle	–
Löschen Sie die Liste der vertrauenswürdigen IP-Adressen oder die Bedrohungslisten	Alle	–	Alle	–
Stellen Sie die Häufigkeit der EventBridge Benachrichtigungen ein	Alle	–	Alle	–

Festlegen des Amazon-S3-Standorts für den Export von Erkenntnissen	Alle	Selbst	Selbst	Selbst
Aktivieren Sie einen oder mehrere optionale Schutzpläne für das gesamte Unternehmen (`ALL`,`NEW`,`NONE`) Dies beinhaltet nicht den Malware-Schutz für S3.	Alle	–	–	–
Aktivieren Sie einen beliebigen GuardDuty Schutzplan für einzelne Konten Dies beinhaltet nicht den Malware-Schutz für EC2 und den Malware-Schutz für S3.	Beliebig	–	Beliebig	–
Malware-Schutz für EC2	Beliebig	–	Selbst	–

Malware-Schutz für EC2 — On-demand Malware-Scan	Beliebig	Selbst	Selbst	Selbst
Malware-Schutz für S3	–	Selbst	–	Selbst
Die Verknüpfung eines Mitglieds kontos aufheben	Irgendein +	–	Beliebig	–
Trennen Sie die Verbindung zu einem Administrator konto	–	–	–	Selbst
Löschen Sie ein getrenntes Mitgliedskonto	Beliebig	–	Beliebig	–
Suspendieren GuardDuty	Irgendein *	–	Irgendein *	–
Deaktiviert GuardDuty	Irgendein *	–	Irgendein *	Selbst

+ Gibt an, dass das delegierte GuardDuty Administratorkonto diese Aktion nur ausführen kann, wenn es die Einstellungen für die automatische Aktivierung für `ALL` die Organisationsmitglieder nicht eingerichtet hat.

* Weist darauf hin, dass ein delegiertes GuardDuty Administratorkonto nicht direkt GuardDuty in einem Mitgliedskonto deaktiviert werden kann. Das Konto eines delegierten GuardDuty Administrators muss zuerst die Verknüpfung mit dem Mitgliedskonto aufheben und es dann löschen. Danach kann jedes Mitgliedskonto GuardDuty in seinen eigenen Konten deaktiviert werden. Weitere Informationen zur Durchführung dieser Aufgaben in Ihrer Organisation finden Sie unter Kontinuierliche Verwaltung Ihrer Mitgliedskonten innerhalb GuardDuty.

Grundlegendes zum Beziehungsstatus der Mitglieder

GuardDuty API-Operationen wie ListMembers und GetMembers geben ein `relationshipStatus` Feld für jedes Mitgliedskonto zurück. Dieses Feld gibt den aktuellen Stand der Beziehung zwischen dem Administratorkonto und dem Mitgliedskonto an. Markieren Sie diesen Wert, wenn Sie bestätigen möchten, dass GuardDuty ein Mitgliedskonto aktiv überwacht wird. Es hilft Ihnen auch bei der Behebung von Gründen, warum das Onboarding eines Mitgliedskontos nicht abgeschlossen wurde oder nicht mehr überwacht wird. In der folgenden Liste werden die möglichen Werte beschrieben.

`Created`

Das Administratorkonto hat dieses Konto als Mitglied hinzugefügt (z. B. durch einen AnrufCreateMembers), aber die Mitgliederbeziehung ist noch nicht aktiv.

`Invited`

Das Administratorkonto hat eine Einladung an dieses Mitgliedskonto gesendet, und die Einladung wartet darauf, angenommen zu werden.

`Enabled`

Dieses Mitgliedskonto ist mit dem Administratorkonto verknüpft und GuardDuty überwacht das Mitgliedskonto aktiv.

`Disabled`

Dieses Mitgliedskonto ist mit dem Administratorkonto verknüpft, überwacht das Mitgliedskonto jedoch GuardDuty nicht aktiv.

`Removed`

Dieses Mitgliedskonto ist nicht mehr mit dem Administratorkonto verknüpft. Dieser Status weist in der Regel darauf hin, dass das Administratorkonto die Verknüpfung entfernt hat.

`Resigned`

Dieses Mitgliedskonto ist nicht mehr mit dem Administratorkonto verknüpft. Dieser Status weist in der Regel darauf hin, dass sich das Mitgliedskonto selbst aus der Assoziation entfernt hat.

`Deleted`

Dieses Mitgliedskonto existiert nicht mehr in GuardDuty.

`EmailVerificationInProgress`

Für die Einladung dieses Mitgliedskontos steht die Überprüfung der E-Mail-Adresse aus.

`EmailVerificationFailed`

Die Einladung dieses Mitgliedskontos hat die Überprüfung der E-Mail-Adresse nicht bestanden.

`RegionDisabled`

Dieses Mitgliedskonto kann nicht überwacht werden, da es GuardDuty nicht aktiviert ist oder in der aktuellen Version nicht verfügbar ist AWS-Region.

`AccountSuspended`

Das Konto dieses Mitglieds AWS-Konto befindet sich in einem gesperrten Zustand.

`CannotCreateDetectorInOrganizationMasterAccount`

GuardDuty kann im AWS Organizations Verwaltungskonto keinen Detektor erstellen, was in der Regel darauf zurückzuführen ist, dass die erforderlichen dienstbezogenen Rollenberechtigungen fehlen.

GuardDuty Konten verwalten mit AWS Organizations

In einer AWS Organisation kann das Verwaltungskonto jedes Konto innerhalb dieser Organisation als delegiertes Administratorkonto festlegen. GuardDuty GuardDuty Wird für dieses Administratorkonto nur im aktuellen Konto automatisch aktiviert. AWS-Region Standardmäßig kann das Administratorkonto GuardDuty für alle Mitgliedskonten in der Organisation in dieser Region aktiviert und verwaltet werden. Das Administratorkonto kann Mitglieder dieser AWS Organisation anzeigen und ihr hinzufügen.

In den folgenden Abschnitten werden Sie durch verschiedene Aufgaben geführt, die Sie als delegiertes GuardDuty Administratorkonto ausführen können.

Inhalt

- Überlegungen und Empfehlungen zur Verwendung mit GuardDuty AWS Organizations
- Für die Benennung eines delegierten GuardDuty Administratorkontos sind Berechtigungen erforderlich
- Benennen eines delegierten Administratorkontos GuardDuty
- Einstellungen für die automatische Aktivierung von Organisationen festlegen
- Mitglieder zur Organisation hinzufügen
- (Optional) Aktivieren Sie Schutzpläne für bestehende Mitgliedskonten
- Kontinuierliche Verwaltung Ihrer Mitgliedskonten innerhalb GuardDuty

- Sperrung GuardDuty für Mitgliedskonto
- Mitgliedskonto vom Administratorkonto trennen (entfernen)
- Mitgliedskonten aus der GuardDuty Organisation löschen
- Das delegierte GuardDuty Administratorkonto ändern

Überlegungen und Empfehlungen zur Verwendung mit GuardDuty AWS Organizations

Die folgenden Überlegungen und Empfehlungen können Ihnen helfen zu verstehen, wie ein delegiertes GuardDuty Administratorkonto funktioniert in GuardDuty:

Ein delegiertes GuardDuty Administratorkonto kann maximal 50.000 Mitglieder verwalten.

Es gibt ein Limit von 50.000 Mitgliedskonten pro delegiertem GuardDuty Administratorkonto. Dies schließt Mitgliedskonten ein, die über die Einladung des Administratorkontos zum Beitritt zu ihrer Organisation hinzugefügt wurden, AWS Organizations oder solche, die die Einladung des GuardDuty Administratorkontos angenommen haben. In Ihrer AWS Organisation kann es jedoch mehr als 50.000 Konten geben.

Wenn Sie das Limit von 50.000 Mitgliedskonten überschreiten, erhalten Sie eine Benachrichtigung von CloudWatch Health Dashboard, und eine E-Mail an das angegebene delegierte GuardDuty Administratorkonto.

Ein delegiertes GuardDuty Administratorkonto ist Regional.

Im Gegensatz AWS Organizations dazu GuardDuty handelt es sich um einen Regionaldienst. Die delegierten GuardDuty Administratorkonten und ihre Mitgliedskonten müssen AWS Organizations in jeder gewünschten Region, in der Sie sie GuardDuty aktiviert haben, hinzugefügt werden. Wenn das Organisationsverwaltungskonto ein delegiertes GuardDuty Administratorkonto nur für USA Ost (Nord-Virginia) festlegt, verwaltet das delegierte GuardDuty Administratorkonto nur Mitgliedskonten, die der Organisation in dieser Region hinzugefügt wurden. Weitere Informationen zur Funktionsparität in Regionen, in denen GuardDuty sie verfügbar ist, finden Sie unter. Regionen und Endpunkte

Sonderfälle für Opt-in-Regionen

- Wenn sich ein delegiertes GuardDuty Administratorkonto von einer Opt-in-Region abmeldet, GuardDuty kann es für kein Mitgliedskonto in der Organisation aktiviert werden, das derzeit deaktiviert ist, auch wenn in Ihrer Organisation die Konfiguration für die GuardDuty

automatische Aktivierung entweder auf nur neue Mitgliedskonten (NEWALL) oder auf alle Mitgliedskonten () eingestellt ist. GuardDuty Informationen zur Konfiguration Ihrer Mitgliedskonten finden Sie im Navigationsbereich der GuardDuty Konsole unter Konten oder verwenden Sie die API. ListMembers

- Wenn Sie mit der Konfiguration für GuardDuty automatische Aktivierung arbeiten, stellen Sie sicherNEW, dass die folgende Reihenfolge eingehalten wird:

  1. Die Mitgliedskonten melden sich für eine Opt-in-Region an.
  2. Fügen Sie die Mitgliedskonten Ihrer Organisation in hinzu. AWS Organizations

  Wenn Sie die Reihenfolge dieser Schritte ändern, funktioniert die Einstellung für die GuardDuty automatische Aktivierung mit NEW in der jeweiligen Opt-in-Region nicht mehr, da das Mitgliedskonto für die Organisation nicht mehr neu ist. GuardDuty bietet zwei alternative Lösungen:

  - Stellen Sie die Konfiguration für die GuardDuty automatische Aktivierung auf einALL, die neue und bestehende Mitgliedskonten einschließt. In diesem Fall ist die Reihenfolge dieser Schritte nicht relevant.
  - Wenn ein Mitgliedskonto bereits Teil Ihrer Organisation ist, verwalten Sie die GuardDuty Konfiguration für dieses Konto individuell in der jeweiligen Opt-in-Region mithilfe der GuardDuty Konsole oder der API.

Erforderlich, damit eine AWS Organisation für alle über dasselbe delegierte GuardDuty Administratorkonto verfügt. AWS-Regionen

Sie müssen ein Mitgliedskonto als delegiertes GuardDuty Administratorkonto für alle aktivierten AWS-Regionen Bereiche GuardDuty festlegen. Wenn Sie beispielsweise ein Mitgliedskonto *111122223333* in angeben*Europe (Ireland)*, können Sie kein anderes Mitgliedskonto in angeben. *555555555555 Canada (Central)* Es ist erforderlich, dass Sie in allen anderen Regionen dasselbe Konto wie das delegierte GuardDuty Administratorkonto verwenden.

Sie können jederzeit ein neues delegiertes GuardDuty Administratorkonto einrichten. Weitere Informationen zum Entfernen des vorhandenen delegierten GuardDuty Administratorkontos finden Sie unter. Das delegierte GuardDuty Administratorkonto ändern

Es wird nicht empfohlen, das Verwaltungskonto Ihrer Organisation als delegiertes GuardDuty Administratorkonto festzulegen.

Das Verwaltungskonto Ihrer Organisation kann das delegierte GuardDuty Administratorkonto sein. Die bewährten AWS -Sicherheitsmethoden folgen jedoch dem Prinzip der geringsten Berechtigung und empfehlen diese Konfiguration nicht.

Durch das Ändern eines delegierten GuardDuty Administratorkontos werden Mitgliedskonten nicht deaktiviert GuardDuty .

> Wenn Sie ein delegiertes GuardDuty Administratorkonto entfernen, werden alle Mitgliedskonten GuardDuty entfernt, die diesem delegierten GuardDuty Administratorkonto zugeordnet sind. GuardDuty bleibt weiterhin für all diese Mitgliedskonten aktiviert.

Für die Benennung eines delegierten GuardDuty Administratorkontos sind Berechtigungen erforderlich

Um GuardDuty mit der Nutzung von Amazon zu beginnen AWS Organizations, bestimmt das AWS Organizations Verwaltungskonto der Organisation ein Konto als delegiertes GuardDuty Administratorkonto. Dies wird GuardDuty als vertrauenswürdiger Service in aktiviert. AWS Organizations Es aktiviert GuardDuty auch das delegierte GuardDuty Administratorkonto und ermöglicht es dem delegierten Administratorkonto, andere Konten in der Organisation in der aktuellen Region zu aktivieren und zu verwalten GuardDuty . Informationen darüber, wie diese Berechtigungen gewährt werden, finden Sie unter Zusammen AWS Organizations mit anderen AWS Diensten verwenden.

Bevor Sie das delegierte GuardDuty Administratorkonto für Ihre Organisation als AWS Organizations Verwaltungskonto festlegen, stellen Sie sicher, dass Sie die folgende GuardDuty Aktion ausführen können:. `guardduty:EnableOrganizationAdminAccount` Mit dieser Aktion können Sie das delegierte GuardDuty Administratorkonto für Ihre Organisation festlegen, indem Sie. GuardDuty Sie müssen außerdem sicherstellen, dass Sie die AWS Organizations Aktionen ausführen dürfen, mit denen Sie Informationen über Ihre Organisation abrufen können.

Um diese Berechtigungen zu gewähren, fügen Sie die folgende Erklärung in eine AWS Identity and Access Management (IAM-) Richtlinie für Ihr Konto ein:

```
{
    "Sid": "PermissionsForGuardDutyAdmin",
    "Effect": "Allow",
    "Action": [
        "guardduty:EnableOrganizationAdminAccount",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
```

```
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
    ],
    "Resource": "*"
}
```

Wenn Sie Ihr AWS Organizations Verwaltungskonto als delegiertes GuardDuty Administratorkonto festlegen möchten, benötigt Ihr Konto auch die IAM-Aktion:. `CreateServiceLinkedRole` Mit dieser Aktion können Sie das Verwaltungskonto initialisieren GuardDuty . Überprüfen Sie dies jedoch, Überlegungen und Empfehlungen zur Verwendung mit GuardDuty AWS Organizations bevor Sie die Berechtigungen hinzufügen.

Um mit der Festlegung des Verwaltungskontos als delegiertes GuardDuty Administratorkonto fortzufahren, fügen Sie der IAM-Richtlinie die folgende Anweisung hinzu und *111122223333* ersetzen Sie sie durch die AWS-Konto ID des Verwaltungskontos Ihrer Organisation:

```
{
 "Sid": "PermissionsToEnableGuardDuty"
 "Effect": "Allow",
 "Action": [
  "iam:CreateServiceLinkedRole"
 ],
 "Resource": "arn:aws:iam::111122223333:role/aws-service-role/guardduty.amazonaws.com/
AWSServiceRoleForAmazonGuardDuty",
 "Condition": {
  "StringLike": {
   "iam:AWSServiceName": "guardduty.amazonaws.com"
  }
 }
}
```

Benennen eines delegierten Administratorkontos GuardDuty

Dieser Abschnitt enthält Schritte zur Benennung eines delegierten Administrators in der Organisation. GuardDuty

Stellen Sie als Verwaltungskonto der AWS Organisation sicher, dass Sie sich die Informationen zur Funktionsweise eines delegierten GuardDuty Administratorkontos durchlesen. Überlegungen und Empfehlungen Bevor Sie fortfahren, stellen Sie sicher, dass Sie Für die Benennung eines delegierten GuardDuty Administratorkontos sind Berechtigungen erforderlich

Wählen Sie eine bevorzugte Zugriffsmethode, um ein delegiertes GuardDuty Administratorkonto für Ihre Organisation festzulegen. Nur ein Verwaltungskonto kann diesen Schritt ausführen.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Um sich anzumelden, verwenden Sie die Anmeldeinformationen für das Verwaltungskonto Ihrer AWS Organizations Organisation.
2. Wählen Sie mithilfe der AWS-Region Auswahltaste in der oberen rechten Ecke der Seite die Region aus, in der Sie das delegierte GuardDuty Administratorkonto für Ihre Organisation festlegen möchten.
3. Führen Sie je nachdem, ob es für Ihr Verwaltungskonto in der aktuellen Region aktiviert GuardDuty ist, einen der folgenden Schritte aus:

   - Falls nicht GuardDuty aktiviert, wählen Sie Amazon GuardDuty — all features und wählen Sie Get started. Diese Aktion führt Sie zur GuardDuty Seite Willkommen auf.
   - Wenn GuardDuty aktiviert, wählen Sie im Navigationsbereich Einstellungen aus.
4. Geben Sie unter Delegierter Administrator die 12-stellige AWS-Konto ID des Kontos ein, das Sie als delegiertes GuardDuty Administratorkonto für die Organisation festlegen möchten.
5. Wählen Sie Delegieren.
6. (Empfohlen) Wiederholen Sie die vorherigen Schritte, um das delegierte GuardDuty Administratorkonto für jedes Konto festzulegen, das Sie aktiviert haben. AWS-Region GuardDuty

API/CLI

1. Führen Sie die Ausführung enableOrganizationAdminAccountmit den Anmeldeinformationen AWS-Konto des Verwaltungskontos der Organisation aus.

   - Alternativ können Sie AWS Command Line Interface dies verwenden. Der folgende AWS CLI Befehl bestimmt ein delegiertes GuardDuty Administratorkonto nur für Ihre aktuelle Region. Führen Sie den folgenden AWS CLI Befehl aus und achten Sie darauf, ihn durch die AWS-Konto ID des Kontos zu *111111111111* ersetzen, das Sie als delegiertes Administratorkonto festlegen möchten: GuardDuty

```
aws guardduty enable-organization-admin-account --admin-account-
id 111111111111
```

Um das delegierte GuardDuty Administratorkonto für andere Regionen festzulegen, geben Sie die Region im Befehl an. AWS CLI Das folgende Beispiel zeigt, wie ein delegiertes GuardDuty Administratorkonto in US West (Oregon) aktiviert wird. Stellen Sie sicher, dass Sie es durch die Region *us-west-2* ersetzen, für die Sie das delegierte GuardDuty Administratorkonto zuweisen möchten.

```
aws guardduty enable-organization-admin-account --admin-account-
id 111111111111 --region us-west-2
```

Informationen darüber, AWS-Regionen wo verfügbar GuardDuty ist, finden Sie unterRegionen und Endpunkte.

Wenn GuardDuty es für Ihr delegiertes GuardDuty Administratorkonto deaktiviert ist, kann es keine Aktion ausführen. Falls dies noch nicht geschehen ist, stellen Sie sicher, dass Sie die Aktivierung GuardDuty für das neu festgelegte delegierte GuardDuty Administratorkonto vorgenommen haben.

2. (Empfohlen) Wiederholen Sie die vorherigen Schritte, um das delegierte GuardDuty Administratorkonto AWS-Region in allen Bereichen festzulegen, die Sie aktiviert haben. GuardDuty

Einstellungen für die automatische Aktivierung von Organisationen festlegen

GuardDuty Mit der Funktion zur automatischen Aktivierung von Organisationen in können Sie in einem einzigen Schritt den gleichen GuardDuty und den Status der Schutzpläne für `ALL` bestehende Konten oder `NEW` Mitgliedskonten in Ihrer Organisation festlegen. In ähnlicher Weise können Sie auch angeben, wann Sie keine Maßnahmen für die Mitgliedskonten ergreifen möchten, indem Sie wählen`NONE`. In den folgenden Schritten werden diese Einstellungen erklärt und es wird auch angegeben, wann Sie eine bestimmte Einstellung verwenden möchten.

> **Note**
>
> Sie können Einstellungen für die automatische Aktivierung für alle Schutzpläne festlegen, mit Ausnahme Malware-Schutz für S3 von.

Wählen Sie eine bevorzugte Zugriffsmethode, um die Einstellungen für die automatische Aktivierung für die Organisation zu aktualisieren.

Console

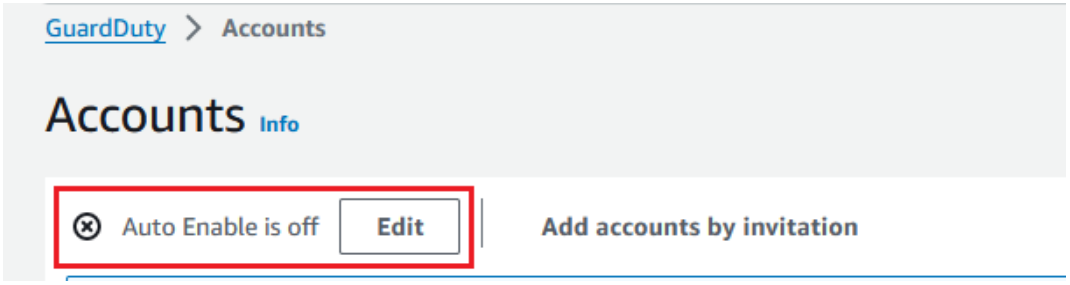
1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

   Verwenden Sie die Anmeldeinformationen des GuardDuty Administratorkontos, um sich anzumelden.

2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.

   Auf der Seite Konten finden Sie Konfigurationsoptionen für das GuardDuty Administratorkonto Auto-enable GuardDuty und die optionalen Schutzpläne für die Mitgliedskonten, die zur Organisation gehören.

3. Um die vorhandenen Einstellungen für die automatische Aktivierung zu aktualisieren, wählen Sie Bearbeiten.



   Dieser Support kann konfiguriert werden, GuardDuty ebenso wie alle unterstützten optionalen Schutzpläne in Ihrem AWS-Region. Sie können im Namen Ihrer Mitgliedskonten eine der folgenden Konfigurationsoptionen auswählen: GuardDuty

   - Für alle Konten aktivieren (**ALL**) — Wählen Sie diese Option, um die entsprechende Option für alle Konten in einer Organisation zu aktivieren. Dazu gehören neue Konten, die der Organisation beitreten, und Konten, die möglicherweise gesperrt oder aus der Organisation entfernt wurden. Dazu gehört auch das delegierte GuardDuty Administratorkonto.

> **Note**
>
> Es kann bis zu 24 Stunden dauern, bis die Konfiguration für alle Mitgliedskonten aktualisiert ist.

- Auto-enable für neue Konten (**`NEW`**) — Wählen Sie aus, GuardDuty ob die optionalen Schutzpläne nur für neue Mitgliedskonten automatisch aktiviert werden sollen, wenn diese Ihrer Organisation beitreten.
- Nicht aktivieren (**`NONE`**) — Wählen Sie diese Option, um zu verhindern, dass die entsprechende Option für neue Konten in Ihrer Organisation aktiviert wird. In diesem Fall verwaltet das GuardDuty Administratorkonto jedes Konto einzeln.

  Wenn Sie die Einstellung für die automatische Aktivierung von `ALL` oder `NEW` auf aktualisieren`NONE`, deaktiviert diese Aktion nicht die entsprechende Option für Ihre vorhandenen Konten. Diese Konfiguration gilt für die neuen Konten, die der Organisation beitreten. Nachdem Sie die Einstellungen für die automatische Aktivierung aktualisiert haben, wird die entsprechende Option für kein neues Konto aktiviert sein.

> **Note**
>
> Wenn sich ein delegiertes GuardDuty Administratorkonto von einer Opt-in-Region abmeldet, GuardDuty kann es für kein Mitgliedskonto in der Organisation aktiviert werden, das derzeit deaktiviert ist, auch wenn in Ihrer Organisation die Konfiguration für die GuardDuty automatische Aktivierung entweder auf nur neue Mitgliedskonten (`NEWALL`) oder auf alle Mitgliedskonten () eingestellt ist. GuardDuty Informationen zur Konfiguration Ihrer Mitgliedskonten finden Sie im Navigationsbereich der GuardDuty Konsole unter Konten oder verwenden Sie die API. ListMembers

4. Wählen Sie Änderungen speichern aus.
5. (Optional) Wenn Sie in jeder Region dieselben Einstellungen verwenden möchten, aktualisieren Sie Ihre Einstellungen in jeder der unterstützten Regionen separat.

   Einige der optionalen Schutzpläne sind möglicherweise nicht überall verfügbar, AWS-Regionen wo sie verfügbar GuardDuty sind. Weitere Informationen finden Sie unter Regionen und Endpunkte.

API/CLI

1. Verwenden Sie UpdateOrganizationConfigurationdie Anmeldeinformationen des delegierten GuardDuty Administratorkontos, um automatisch optionale Schutzpläne in dieser Region für Ihr Unternehmen zu konfigurieren GuardDuty . Informationen zu den verschiedenen Konfigurationen für die automatische Aktivierung finden Sie unter Auto EnableOrganizationMembers.

   Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

   Um die Einstellungen für die automatische Aktivierung für einen der unterstützten optionalen Schutzpläne in Ihrer Region festzulegen, folgen Sie den Schritten in den entsprechenden Dokumentationsabschnitten der einzelnen Schutzpläne.

2. Sie können die Einstellungen für Ihre Organisation in der aktuellen Region überprüfen. Führen Sie describeOrganizationConfiguration. Stellen Sie sicher, dass Sie die Melder-ID des delegierten GuardDuty Administratorkontos angeben.

   > **Note**
   >
   > Die Aktualisierung der Konfiguration aller Mitgliedskonten kann bis zu 24 Stunden dauern.

3. Führen Sie alternativ den folgenden AWS CLI Befehl aus, um die Einstellungen so festzulegen, dass GuardDuty in dieser Region automatisch neue Konten (`NEW`), die der Organisation beitreten, alle Konten (`ALL`) oder keines der Konten (`NONE`) in der Organisation aktiviert oder deaktiviert werden. Weitere Informationen finden Sie unter Auto EnableOrganizationMembers. Je nach Ihren Einstellungen müssen Sie möglicherweise `NEW` durch `ALL` oder `NONE` ersetzen. Wenn Sie den Schutzplan mit konfigurieren`ALL`, wird der Schutzplan auch für das delegierte GuardDuty Administratorkonto aktiviert. Stellen Sie sicher, dass Sie die Melder-ID des delegierten GuardDuty Administratorkontos angeben, das die Organisationskonfiguration verwaltet.

   Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members=NEW
```

4. Sie können die Einstellungen für Ihre Organisation in der aktuellen Region überprüfen. Führen Sie den folgenden AWS CLI Befehl aus, indem Sie die Detektor-ID des delegierten GuardDuty Administratorkontos verwenden.

```
aws guardduty describe-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0
```

(Empfohlen) Wiederholen Sie die vorherigen Schritte in jeder Region, indem Sie die Detektor-ID für das delegierte GuardDuty Administratorkonto verwenden.

> **Note**
>
> Wenn sich ein delegiertes GuardDuty Administratorkonto von einer Opt-in-Region abmeldet, GuardDuty kann es für kein Mitgliedskonto in der Organisation aktiviert werden, das derzeit deaktiviert ist, auch wenn in Ihrer Organisation die Konfiguration für die GuardDuty automatische Aktivierung entweder auf nur neue Mitgliedskonten (`NEWALL`) oder auf alle Mitgliedskonten () eingestellt ist. GuardDuty Informationen zur Konfiguration Ihrer Mitgliedskonten finden Sie im Navigationsbereich der GuardDuty Konsole unter Konten oder verwenden Sie die API. ListMembers

Mitglieder zur Organisation hinzufügen

Als delegiertes GuardDuty Administratorkonto können Sie der GuardDuty Organisation ein oder mehrere AWS-Konten Konten hinzufügen. Wenn Sie ein Konto als GuardDuty Mitglied hinzufügen, wird es automatisch in dieser Region GuardDuty aktiviert. Es gibt eine Ausnahme für das Organisationsverwaltungskonto. Bevor das Verwaltungskonto als GuardDuty Mitglied hinzugefügt werden kann, muss es GuardDuty aktiviert worden sein.

Wählen Sie eine bevorzugte Methode, um Ihrer GuardDuty Organisation ein Mitgliedskonto hinzuzufügen.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Verwenden Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto, um sich anzumelden.

2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.

   In der Kontentabelle werden alle Mitgliedskonten angezeigt, die aktiv (nicht gesperrt AWS-Konten) sind und möglicherweise dem delegierten GuardDuty Administratorkonto zugeordnet sind. Wenn das Mitgliedskonto mit dem Administratorkonto der Organisation verknüpft ist, ist der Typ einer der folgenden: Über Organizations oder Auf Einladung. Wenn ein Mitgliedskonto nicht mit dem GuardDuty Administratorkonto der Organisation verknüpft ist, lautet der Typ dieses Mitgliedskontos Kein Mitglied.

3. Wählen Sie eine oder mehrere Konto-IDs aus, die Sie als Mitglieder hinzufügen möchten. Diese Konto-IDs müssen den Typ Über Organisationen haben.

   Konten, die auf Einladung hinzugefügt werden, gehören nicht zu Ihrer Organisation. Sie können solche Konten einzeln verwalten. Weitere Informationen finden Sie unter Verwalten von Konten auf Einladung.

4. Wählen Sie das Drop-down-Menü Aktionen und dann Mitglied hinzufügen aus. Nachdem Sie dieses Konto als Mitglied hinzugefügt haben, gilt die GuardDuty Konfiguration für die automatische Aktivierung. Je nach den Einstellungen in kann Einstellungen für die automatische Aktivierung von Organisationen festlegen sich die GuardDuty Konfiguration dieser Konten ändern.

5. Sie können den Abwärtspfeil in der Spalte Status auswählen, um die Konten nach dem Status Kein Mitglied zu sortieren, und dann jedes Konto auswählen, das in der aktuellen Region nicht GuardDuty aktiviert wurde.

   Wenn noch keines der in der Kontentabelle aufgelisteten Konten als Mitglied hinzugefügt wurde, können Sie es GuardDuty in der aktuellen Region für alle Organisationskonten aktivieren. Wählen Sie im Banner oben auf der Seite Aktivieren aus. Diese Aktion aktiviert automatisch die Auto-enable GuardDuty Konfiguration, sodass sie für jedes neue Konto aktiviert GuardDuty wird, das der Organisation beitritt.

6. Wählen Sie Bestätigen, um die Konten als Mitglieder hinzuzufügen. Diese Aktion ist auch GuardDuty für alle ausgewählten Konten aktiviert. Der Status für die eingeladenen Konten ändert sich in Aktiviert.

7. (Empfohlen) Wiederholen Sie diese Schritte in jedem Schritt AWS-Region. Dadurch wird sichergestellt, dass das delegierte GuardDuty Administratorkonto Ergebnisse und andere Konfigurationen für Mitgliedskonten in allen Regionen verwalten kann, in denen Sie die GuardDuty Aktivierung aktiviert haben.

   Die automatische Aktivierungsfunktion ist GuardDuty für alle future Mitglieder Ihrer Organisation aktiviert. Auf diese Weise kann Ihr delegiertes GuardDuty Administratorkonto alle neuen Mitglieder verwalten, die innerhalb der Organisation erstellt wurden oder der Organisation hinzugefügt werden. Wenn die Anzahl der Mitgliedskonten das Limit von 50.000 erreicht, wird die Auto-enable Funktion automatisch deaktiviert. Wenn Sie ein Mitgliedskonto entfernen und die Gesamtzahl der Mitglieder auf weniger als 50.000 sinkt, wird die Auto-enable Funktion wieder aktiviert.

API/CLI

- Führen Sie CreateMembersdie Ausführung mit den Anmeldeinformationen des delegierten GuardDuty Administratorkontos aus.

  Sie müssen die Regional Detector-ID des delegierten GuardDuty Administratorkontos und die Kontodetails (AWS-Konto IDs und entsprechende E-Mail-Adressen) der Konten angeben, die Sie als GuardDuty Mitglieder hinzufügen möchten. Sie können mit dieser API-Operation ein oder mehrere Mitglieder erstellen.

  Wenn Sie CreateMembers in Ihrer Organisation aktiv sind, gelten die Einstellungen für die automatische Aktivierung für neue Mitglieder, sobald neue Mitgliedskonten Ihrer Organisation beitreten. Wenn Sie CreateMembers mit einem bestehenden Mitgliedskonto arbeiten, gilt die Organisationskonfiguration auch für die vorhandenen Mitglieder. Dies könnte die aktuelle Konfiguration der vorhandenen Mitgliedskonten ändern.

  Führen Sie ListAccountsdie AWS Organizations API-Referenz aus, um alle Konten in der AWS Organisation anzuzeigen.

  - Alternativ können Sie verwenden AWS Command Line Interface. Führen Sie den folgenden AWS CLI -Befehl aus und stellen Sie sicher, dass Sie Ihre eigene gültige Detektor-ID und die mit der AWS-Konto -ID verknüpfte E-Mail-Adresse verwenden.

    Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

```
aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-details AccountId=111122223333,Email=guardduty-member-
name@amazon.com
```

Sie können eine Liste aller Organisationsmitglieder anzeigen, indem Sie den folgenden AWS CLI Befehl ausführen:

```
aws organizations list-accounts
```

Nachdem Sie dieses Konto als Mitglied hinzugefügt haben, gilt die GuardDuty Konfiguration für die automatische Aktivierung.

(Optional) Aktivieren Sie Schutzpläne für bestehende Mitgliedskonten

Das folgende Verfahren umfasst Schritte zum Aktivieren von Schutzplänen für bestehende Mitgliedskonten mithilfe der Kontoseite. Die Schritte dazu mithilfe der API oder AWS CLI finden Sie in den Dokumenten zum jeweiligen Schutzplan.

Auf der Seite Konten können Sie Schutzpläne für einzelne Konten aktivieren.

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Verwenden Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto.
2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
3. Wählen Sie das Konto aus, für das Sie einen Schutzplan konfigurieren möchten. Wiederholen Sie die folgenden Schritte für jeden Schutzplan, den Sie konfigurieren möchten:

   a. Wählen Sie Schutzpläne bearbeiten aus.

   b. Wählen Sie aus der Liste der Schutzpläne einen Schutzplan aus, den Sie konfigurieren möchten.

   c. Wählen Sie eine der Aktionen aus, die Sie für diesen Schutzplan ausführen möchten, und klicken Sie dann auf Bestätigen.

   d. Für das ausgewählte Konto wird in der Spalte, die dem konfigurierten Schutzplan entspricht, die aktualisierte Konfiguration als Aktiviert oder Nicht aktiviert angezeigt.

Kontinuierliche Verwaltung Ihrer Mitgliedskonten innerhalb GuardDuty

Als delegiertes GuardDuty Administratorkonto sind Sie dafür verantwortlich, die Konfiguration GuardDuty und die optionalen Schutzpläne für alle Konten in Ihrer Organisation in allen unterstützten Konten aufrechtzuerhalten. AWS-Region In den folgenden Abschnitten finden Sie die Optionen zur Beibehaltung des Konfigurationsstatus der optionalen Schutzpläne GuardDuty oder der zugehörigen optionalen Schutzpläne:

Um den Konfigurationsstatus Ihrer gesamten Organisation in jeder Region aufrechtzuerhalten

- Legen Sie mithilfe der GuardDuty Konsole Einstellungen für die automatische Aktivierung für die gesamte Organisation fest — Sie können die GuardDuty automatische Aktivierung entweder für alle (`ALL`) Mitglieder der Organisation oder für neue (`NEW`) Mitglieder, die der Organisation beitreten, aktivieren oder festlegen, dass (`NONE`) keines der Mitglieder der Organisation automatisch aktiviert wird.

  Sie können auch dieselben oder unterschiedliche Einstellungen für alle darin enthaltenen Schutzpläne konfigurieren. GuardDuty

  Es kann bis zu 24 Stunden dauern, bis die Konfiguration für alle Mitgliedskonten in der Organisation aktualisiert ist.
- Aktualisieren Sie die Einstellungen für die automatische Aktivierung mithilfe von API — Run UpdateOrganizationConfiguration, um die automatische Konfiguration GuardDuty und die optionalen Schutzpläne für das Unternehmen zu konfigurieren. Wenn Sie ausführen CreateMembers, um neue Mitgliedskonten in Ihrer Organisation hinzuzufügen, werden die konfigurierten Einstellungen automatisch angewendet. Wenn Sie CreateMembers mit einem vorhandenen Mitgliedskonto arbeiten, gilt die Organisationskonfiguration auch für die vorhandenen Mitglieder. Dies könnte die aktuelle Konfiguration der vorhandenen Mitgliedskonten ändern.

  Um alle Konten in Ihrer Organisation anzuzeigen, führen Sie ListAccountsden Befehl AWS Organizations API-Referenz aus.

Um den Konfigurationsstatus für Mitgliedskonten in jeder Region einzeln beizubehalten

- Um alle Konten in Ihrer Organisation anzuzeigen, führen Sie ListAccountsden Befehl AWS Organizations API-Referenz aus.
- Wenn Sie möchten, dass ausgewählte Mitgliedskonten einen anderen Konfigurationsstatus haben, führen Sie den Vorgang UpdateMemberDetectorsfür jedes Mitgliedskonto einzeln aus.

Sie können dieselbe Aufgabe mit der GuardDuty Konsole ausführen, indem Sie in der GuardDuty Konsole zur Seite Konten navigieren.

Informationen zur Aktivierung von Schutzplänen für einzelne Konten mithilfe der Konsole oder der API finden Sie auf der Konfigurationsseite für den entsprechenden Schutzplan.

Sperrung GuardDuty für Mitgliedskonto

Als delegiertes GuardDuty Administratorkonto können Sie den GuardDuty Dienst für ein Mitgliedskonto in Ihrer Organisation sperren. Wenn Sie dies tun, verbleibt das Mitgliedskonto weiterhin in Ihrer GuardDuty Organisation. Sie können es GuardDuty für diese Mitgliedskonten auch zu einem späteren Zeitpunkt wieder aktivieren. Wenn Sie dieses Mitgliedskonto jedoch irgendwann trennen (entfernen) möchten, müssen Sie, nachdem Sie die Schritte in diesem Abschnitt ausgeführt haben, die Schritte unter befolgen. Mitgliedskonto vom Administratorkonto trennen (entfernen)

Wenn Sie ein Mitgliedskonto sperren GuardDuty , können Sie mit den folgenden Änderungen rechnen:

- GuardDuty überwacht nicht mehr die Sicherheit der AWS Umwelt oder generiert neue Erkenntnisse.
- Die vorhandenen Ergebnisse im Mitgliedskonto bleiben erhalten.
- Für ein GuardDuty gesperrtes Mitgliedskonto fallen keine Gebühren an. GuardDuty

  Wenn das Mitgliedskonto Malware Protection for S3 für einen oder mehrere Buckets in seinem Konto aktiviert hat, hat die Sperrung GuardDuty keine Auswirkungen auf die Konfiguration von Malware Protection for S3. Für das Mitgliedskonto fallen weiterhin die Nutzungskosten für Malware Protection for S3 an. Damit das Mitgliedskonto Malware Protection for S3 nicht mehr nutzen kann, muss es diese Funktion für die geschützten Buckets deaktivieren. Weitere Informationen finden Sie unter Malware-Schutz für S3 für einen geschützten Bucket deaktivieren.

Wählen Sie eine bevorzugte Methode GuardDuty zur Sperrung eines Mitgliedskontos in Ihrer Organisation.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

Verwenden Sie zur Anmeldung die Anmeldeinformationen des delegierten GuardDuty Administratorkontos.

2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
3. Wählen Sie auf der Seite Konten ein oder mehrere Konten aus, für die Sie eine Sperrung vornehmen möchten. GuardDuty
4. Wählen Sie das Dropdownmenü „Aktionen“ und dann „ GuardDutySperren“.
5. Wählen Sie „Sperren“ GuardDuty, um die Auswahl zu bestätigen.

   Dadurch wird der Status des Mitgliedskontos auf Deaktiviert (gesperrt) geändert.

   Wiederholen Sie die vorherigen Schritte in jeder weiteren Region, in der Sie die Zuordnung zum Mitgliedskonto aufheben oder entfernen möchten.

API

1. Verwenden Sie die ListMembersAPI, um die Konto-ID des Mitgliedskontos abzurufen GuardDuty, für das Sie die Sperre sperren möchten. Nehmen Sie den `OnlyAssociated` Parameter in Ihre Anfrage auf. Wenn Sie den Wert dieses Parameters auf setzen`true`, wird ein `members` Array GuardDuty zurückgegeben, das nur Details zu den Konten enthält, die derzeit GuardDuty Mitglieder sind.

   Alternativ können Sie AWS Command Line Interface (AWS CLI) verwenden, um den folgenden Befehl auszuführen:

   ```
   aws guardduty list-members --only-associated true --region us-east-1
   ```

   Ersetzen Sie es *`us-east-1`* durch die Region, in der Sie GuardDuty das Konto sperren möchten.
2. Um ein oder mehrere GuardDuty Mitgliedskonten StopMonitoringMemberszu sperren, führe den Befehl Sperren GuardDuty für ein Mitgliedskonto aus.

   Alternativ können Sie AWS CLI den folgenden Befehl ausführen:

   ```
   aws guardduty stop-monitoring-members --detector-id
    12abc34d567e8fa901bc2d34EXAMPLE --account-ids 111122223333 --region us-east-1
   ```

Ersetzen Sie es `us-east-1` durch die Region, in der Sie dieses Konto sperren möchten. Wenn Sie eine Liste mit Konto-IDs haben, die Sie entfernen möchten, trennen Sie sie durch ein Leerzeichen.

Wenn Sie die Zuordnung zu diesem Mitgliedskonto weiter aufheben (entfernen) möchten, folgen Sie den Schritten unterMitgliedskonto vom Administratorkonto trennen (entfernen).

Mitgliedskonto vom Administratorkonto trennen (entfernen)

Wenn Sie die Konfiguration der GuardDuty Einstellungen und den Zugriff auf die Daten eines Mitgliedskontos beenden möchten, entfernen Sie dieses Konto als GuardDuty Mitgliedskonto. Sie können dies tun, indem Sie dieses Konto vom GuardDuty Administratorkonto trennen (entfernen).

Wenn Sie die Zuordnung zu einem GuardDuty Mitgliedskonto aufheben, passiert Folgendes:

- GuardDuty bleibt für das aktuelle Konto aktiviert AWS-Region, aber das Konto wird vom GuardDuty delegierten Administratorkonto getrennt.
- Das getrennte Konto wird weiterhin im Kontoinventar angezeigt.
- Das GuardDuty Administratorkonto hat keinen Zugriff mehr auf die Ergebnisse dieses eigenständigen Kontos.
- Der Kontoinhaber wird nicht über die Trennung der Verbindung informiert.

Sie können das getrennte Konto zu einem späteren Zeitpunkt wieder zu Ihrer Organisation hinzufügen.

Wählen Sie eine bevorzugte Methode, um ein Mitgliedskonto von Ihrer Organisation zu trennen (zu entfernen).

Console

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

   Verwenden Sie zur Anmeldung die Anmeldeinformationen des delegierten GuardDuty Administratorkontos.
2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
3. In der Tabelle Konten können Sie ein Konto entfernen, dessen Typ auf Via Organizations und der Status auf Aktiviert gesetzt ist.

Wählen Sie ein oder mehrere Konten mit demselben Typ und Status aus.

4. Wählen Sie im Dropdownmenü Aktionen die Option Konto trennen aus.
5. Wählen Sie Konto trennen, um Ihre Auswahl zu bestätigen.
6. Der Statuswert für die ausgewählten Konten wird auf Kein Mitglied geändert. Die Anzahl der Via-Organisationen (Active/All) in der oberen rechten Ecke der Kontoseite ändert sich entsprechend der Aktualisierung.

   Wiederholen Sie die vorherigen Schritte in jeder weiteren Region, in der Sie die Zuordnung zum Mitgliedskonto aufheben möchten.

API

1. Verwenden Sie die ListMembersAPI, um die Konto-ID für das Mitgliedskonto abzurufen, das Sie entfernen möchten. Nehmen Sie den `OnlyAssociated` Parameter in Ihre Anfrage auf. Wenn Sie den Wert dieses Parameters auf setzen`true`, wird ein `members` Array GuardDuty zurückgegeben, das nur Details zu den Konten enthält, die derzeit GuardDuty Mitglieder sind.

   Alternativ können Sie AWS Command Line Interface (AWS CLI) verwenden, um den folgenden Befehl auszuführen:

   ```
   aws guardduty list-members --only-associated true --region us-east-1
   ```

   Ersetzen Sie es *`us-east-1`* durch die Region, aus der Sie dieses Konto entfernen möchten.
2. Um ein oder mehrere GuardDuty Mitgliedskonten zu entfernen, führen Sie den Befehl DisassociateMemberszum Entfernen des Mitgliedskontos aus, das dem Administratorkonto zugeordnet ist.

   Alternativ können Sie AWS CLI den folgenden Befehl ausführen:

   ```
   aws guardduty disassociate-members --detector-id 12abc34d567e8fa901bc2d34EXAMPLE
    --account-ids 111122223333 --region us-east-1
   ```

   Ersetzen Sie es *`us-east-1`* durch die Region, aus der Sie dieses Konto entfernen möchten. Wenn Sie eine Liste mit Konto-IDs haben, die Sie entfernen möchten, trennen Sie sie durch ein Leerzeichen.

Mitgliedskonten aus der GuardDuty Organisation löschen

Als delegiertes GuardDuty Administratorkonto können Sie, nachdem Sie die Zuordnung zu einem Mitgliedskonto aufgehoben haben und dieses Mitgliedskonto nicht mehr in der GuardDuty Organisation behalten möchten, dieses Mitgliedskonto aus Ihrer GuardDuty Organisation löschen. Dieses Mitgliedskonto wird nicht mehr in Ihrem Kontoinventar angezeigt. Wenn es in diesem Mitgliedskonto jedoch nicht gesperrt GuardDuty wurde, bleiben die Konfiguration GuardDuty und die speziellen Schutzpläne unverändert. Dieses Konto wird nun zu einem eigenständigen Konto und kann GuardDuty sich selbst deaktivieren.

Durch diesen Schritt wird das Mitgliedskonto nicht aus Ihrer AWS Organisation gelöscht.

Wählen Sie eine bevorzugte Methode, um ein Mitgliedskonto aus Ihrer GuardDuty Organisation zu löschen.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Verwenden Sie zur Anmeldung die Anmeldeinformationen des delegierten GuardDuty Administratorkontos.
2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
3. In der Tabelle Konten können Sie ein Konto entfernen, dessen Typ die Option Über Organizations und den Status Entfernt (getrennt) hat.

   Wählen Sie ein oder mehrere Konten mit demselben Typ und Status aus.
4. Wählen Sie im Dropdownmenü Aktionen die Option Konto löschen aus.
5. Wählen Sie Konten löschen, um Ihre Auswahl zu bestätigen. Das ausgewählte Kontomitglied wird nicht mehr in Ihrer Kontentabelle angezeigt.

   Wiederholen Sie die vorherigen Schritte in jeder weiteren Region, in der Sie dieses Mitgliedskonto löschen möchten.

API/CLI

1. Verwenden Sie die ListMembersAPI, um die Konto-ID für das Mitgliedskonto abzurufen, das Sie löschen möchten. Nehmen Sie den `OnlyAssociated` Parameter in Ihre Anfrage auf. Wenn Sie den Wert dieses Parameters auf setzen, wird ein `members` Array GuardDuty

zurückgegeben`false`, das nur Details zu den Konten enthält, bei denen es sich derzeit um GuardDuty Mitglieder handelt, deren Zuordnung aufgehoben wurde.

Alternativ können Sie AWS Command Line Interface (AWS CLI) verwenden, um den folgenden Befehl auszuführen:

```
aws guardduty list-members --detector-id 12abc34d567e8fa901bc2d34EXAMPLE --only-associated="false" --region us-east-1
```

*12abc34d567e8fa901bc2d34EXAMPLE*Ersetzen Sie es durch die Erkennungs-ID für das delegierte GuardDuty Administratorkonto und *us-east-1* durch die Region, aus der Sie dieses Konto entfernen möchten.

2. Um ein oder mehrere GuardDuty Mitgliedskonten zu löschen, führen Sie den DeleteMembersBefehl zum Löschen des Mitgliedskontos aus der GuardDuty Organisation aus.

   Alternativ können Sie AWS CLI den folgenden Befehl ausführen:

   ```
   aws guardduty delete-members --detector-id 12abc34d567e8fa901bc2d34EXAMPLE --account-ids 111122223333 --region us-east-1
   ```

   *12abc34d567e8fa901bc2d34EXAMPLE*Ersetzen Sie es durch die Erkennungs-ID für das delegierte GuardDuty Administratorkonto und *us-east-1* durch die Region, aus der Sie dieses Konto entfernen möchten. Wenn Sie eine Liste mit Konto-IDs haben, die Sie entfernen möchten, trennen Sie sie durch ein Leerzeichen.

Das delegierte GuardDuty Administratorkonto ändern

Sie können das delegierte GuardDuty Administratorkonto für Ihre Organisation in jeder Region entfernen und dann in jeder Region einen neuen Administrator delegieren. Um die Sicherheit der Mitgliedskonten Ihrer Organisation in einer Region aufrechtzuerhalten, benötigen Sie in dieser Region ein delegiertes GuardDuty Administratorkonto.

> **Hinweis**
>
> Bevor Sie ein delegiertes GuardDuty Administratorkonto entfernen, müssen Sie die Zuordnung aller Mitgliedskonten, die dem delegierten GuardDuty Administratorkonto

zugeordnet sind, aufheben und sie anschließend aus der Organisation löschen. GuardDuty Weitere Informationen zu diesen Schritten finden Sie in den folgenden Dokumenten:

- Mitgliedskonto vom Administratorkonto trennen (entfernen)
- Mitgliedskonten aus der GuardDuty Organisation löschen

Bestehendes delegiertes GuardDuty Administratorkonto wird entfernt

Schritt 1 — Um ein vorhandenes delegiertes GuardDuty Administratorkonto in jeder Region zu entfernen

1. Führen Sie als vorhandenes delegiertes GuardDuty Administratorkonto alle Mitgliedskonten auf, die mit Ihrem Administratorkonto verknüpft sind. Führen Sie ListMembersmit`OnlyAssociated=false`.
2. Wenn die Einstellung Automatische Aktivierung für GuardDuty oder einen der optionalen Schutzpläne auf gesetzt ist, führen Sie den Befehl aus`ALL`, UpdateOrganizationConfigurationum die Organisationskonfiguration entweder auf `NEW` oder `NONE` zu aktualisieren. Diese Aktion verhindert, dass ein Fehler auftritt, wenn Sie im nächsten Schritt die Verknüpfung aller Mitgliedskonten aufheben.
3. Führen Sie aus DisassociateMembers, um die Zuordnung aller Mitgliedskonten aufzuheben, die dem Administratorkonto zugeordnet sind.
4. Führen Sie aus DeleteMembers, um die Verknüpfungen zwischen dem Administratorkonto und den Mitgliedskonten zu löschen.
5. Führen Sie als Organisationsverwaltungskonto aus, DisableOrganizationAdminAccountum das vorhandene delegierte GuardDuty Administratorkonto zu entfernen.
6. Wiederholen Sie diese Schritte in allen Bereichen, in AWS-Region denen Sie über dieses delegierte GuardDuty Administratorkonto verfügen.

Schritt 2 — So heben Sie die Registrierung eines bestehenden delegierten Administratorkontos auf GuardDuty AWS Organizations (One-time globale Aktion)

- Führen Sie DeregisterDelegatedAdministratordie AWS Organizations API-Referenz aus, um das bestehende delegierte GuardDuty Administratorkonto in abzumelden. AWS Organizations

  Alternativ können Sie den folgenden AWS CLI Befehl ausführen:

```
aws organizations deregister-delegated-administrator --account-id 111122223333 --
service-principal guardduty.amazonaws.com
```

Stellen Sie sicher, dass Sie es *111122223333* durch das vorhandene delegierte GuardDuty Administratorkonto ersetzen.

Nachdem Sie das alte delegierte GuardDuty Administratorkonto abgemeldet haben, können Sie es dem neuen delegierten GuardDuty Administratorkonto als Mitgliedskonto hinzufügen.

Benennen eines neuen delegierten GuardDuty Administratorkontos in jeder Region

1. Weisen Sie in jeder Region ein neues delegiertes GuardDuty Administratorkonto zu, indem Sie Ihre bevorzugte Zugriffsmethode verwenden: GuardDuty Konsole oder API oder. AWS CLI Weitere Informationen finden Sie unter Benennen eines delegierten Administratorkontos GuardDuty.
2. Führen Sie den DescribeOrganizationConfigurationBefehl aus, um die aktuelle Konfiguration für die automatische Aktivierung für Ihre Organisation anzuzeigen.

> **Important**
>
> Bevor Sie dem neuen delegierten GuardDuty Administratorkonto Mitglieder hinzufügen, müssen Sie die Konfiguration für die automatische Aktivierung für Ihre Organisation überprüfen. Diese Konfiguration ist spezifisch für das neue delegierte GuardDuty Administratorkonto und die ausgewählte Region und bezieht sich nicht auf. AWS Organizations Wenn Sie (ein neues oder ein vorhandenes) Mitgliedskonto einer Organisation unter dem neuen delegierten GuardDuty Administratorkonto hinzufügen, gilt die automatische Aktivierungskonfiguration des neuen delegierten GuardDuty Administratorkontos zum Zeitpunkt der Aktivierung GuardDuty oder eines seiner optionalen Schutzpläne.

Ändern Sie die Organisationskonfiguration für das neue delegierte GuardDuty Administratorkonto mithilfe Ihrer bevorzugten Zugriffsmethode — GuardDuty Konsole oder API oder. AWS CLI Weitere Informationen finden Sie unter Einstellungen für die automatische Aktivierung von Organisationen festlegen.

GuardDuty Konten auf Einladung verwalten

Um Konten außerhalb Ihrer Organisation zu verwalten, können Sie die Legacy-Einladungsmethode verwenden. Wenn Sie diese Methode verwenden, wird Ihr Konto als Administratorkonto designiert, wenn ein anderes Konto Ihre Einladung annimmt, ein Mitgliedskonto zu werden.

> **Note**
>
> GuardDuty empfiehlt, Ihre Mitgliedskonten AWS Organizations anstelle von GuardDuty Einladungen zu verwalten. Weitere Informationen finden Sie unter Verwalten von Konten mit AWS Organizations.

Wenn es sich bei Ihrem Konto nicht um ein Administratorkonto handelt, können Sie eine Einladung von einem anderen Konto annehmen. In diesem Fall wird Ihr Konto ein Mitgliedskonto. Ein AWS Konto kann nicht gleichzeitig GuardDuty Administratorkonto und Mitgliedskonto sein.

Wenn Sie eine Einladung von einem Konto annehmen, können Sie keine Einladung von einem anderen Konto annehmen. Um eine Einladung von einem anderen Konto anzunehmen, müssen Sie zunächst die Verbindung zwischen Ihrem Konto und dem vorhandenen Administratorkonto trennen. Alternativ kann das Administratorkonto auch die Zuordnung Ihres Kontos zu seiner Organisation aufheben und es daraus entfernen.

Konten, die per Einladung verknüpft wurden, haben eine ähnliche allgemeine Beziehung zwischen Administratorkonto und Mitglied wie Konten, die von verknüpft sind AWS Organizations, wie unter beschrieben. Grundlegendes zur Beziehung zwischen GuardDuty Administratorkonto und Mitgliedskonten Benutzer mit Administratorkonten für Einladungen können jedoch nicht im Namen GuardDuty der zugehörigen Mitgliedskonten aktivieren oder andere Konten innerhalb ihrer Organisation einsehen, die keine Mitglieder sind. AWS Organizations

> **Important**
>
> Cross-regional Bei GuardDuty der Erstellung von Mitgliedskonten mit dieser Methode kann es zu einer Datenübertragung kommen. GuardDuty verwendet zur Überprüfung der E-Mail-Adressen von Mitgliedskonten einen E-Mail-Bestätigungsdienst, der nur in der Region USA Ost (Nord-Virginia) verfügbar ist.

Themen

- Konten auf Einladung hinzufügen
- Konsolidierung von GuardDuty Administratorkonten unter einer einzigen Organisation

Konten auf Einladung hinzufügen

Als Administratorkonto, das bereits GuardDuty aktiviert wurde, können Sie Mitglieder hinzufügen, um mit der Nutzung zu beginnen GuardDuty. Nachdem Sie die Mitglieder hinzugefügt haben, können Sie sie zum Beitritt einladen GuardDuty, und sie können wählen, ob sie auf Ihre Einladung antworten möchten.

> **Note**
>
> GuardDuty empfiehlt, Ihre Mitgliedskonten AWS Organizations anstelle von GuardDuty Einladungen zu verwalten. Weitere Informationen finden Sie unter Verwalten von Konten mit AWS Organizations.

Wählen Sie eine bevorzugte Zugriffsmethode, um GuardDuty Mitgliedskonten als GuardDuty Administratorkonto hinzuzufügen.

Console

Schritt 1: Konto hinzufügen

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
3. Wählen Sie im oberen Bereich Konten auf Einladung hinzufügen aus.
4. Geben Sie auf der Seite Mitgliedskonten hinzufügen unter Kontendetails eingeben die AWS-Konto -ID und E-Mail-Adresse des Kontos ein, das Sie hinzufügen möchten.
5. Um eine weitere Zeile hinzuzufügen, in der die Kontodetails nacheinander eingegeben werden können, wählen Sie Weiteres Konto hinzufügen. Sie können auch CSV-Datei mit Kontodetails hochladen wählen, um mehrere Konten gleichzeitig hinzuzufügen.

> **Important**
>
> Die erste Zeile Ihrer CSV-Datei muss wie im folgenden Beispiel den folgenden Header enthalten – `Account ID,Email`. Jede nachfolgende Zeile muss eine

einzige gültige AWS-Konto ID und die zugehörige E-Mail-Adresse enthalten. Das Format einer Zeile ist gültig, wenn sie nur eine AWS-Konto -ID und die zugehörige E-Mail-Adresse enthält, die durch ein Komma getrennt sind.

```
Account ID,Email
                                555555555555,user@example.com
```

6. Nachdem Sie alle Kontodetails hinzugefügt haben, wählen Sie Weiter. Sie können die neu hinzugefügten Konten in der Tabelle Konten einsehen. Der Status dieser Konten lautet Einladung nicht gesendet. Informationen zum Senden einer Einladung an ein oder mehrere hinzugefügte Konten finden Sie unter Step 2 - Invite an account.

Schritt 2: Ein Konto einladen

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
3. Wählen Sie ein oder mehrere Konten aus, die Sie zu Amazon einladen möchten GuardDuty.
4. Wählen Sie im Drop-down-Menü Aktionen und dann Einladen aus.
5. Geben Sie im GuardDuty Dialogfeld „Einladung zu“ eine (optionale) Einladungsnachricht ein.

   Wenn das eingeladene Konto keinen Zugriff auf E-Mails hat, aktivieren Sie das Kontrollkästchen Außerdem eine E-Mail-Benachrichtigung an den Root-Benutzer der eingeladenen Person senden AWS-Konto und in der Liste der eingeladenen Person eine Benachrichtigung generieren. AWS Health Dashboard
6. Wählen Sie Send invitation (Einladung senden) aus. Wenn die eingeladenen Personen Zugriff auf die angegebene E-Mail-Adresse haben, können sie sich die Einladung ansehen, indem sie die Konsole unter öffnen. GuardDuty https://console.aws.amazon.com/guardduty/
7. Wenn ein Eingeladener die Einladung annimmt, ändert sich der Wert in der Spalte Status in Eingeladen. Weitere Informationen zur Annahme einer Einladung finden Sie unter Step 3 - Accept an invitation.

Schritt 3: Eine Einladung annehmen

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

> **Important**
>
> Sie müssen sie aktivieren, GuardDuty bevor Sie eine Mitgliedschaftseinladung anzeigen oder annehmen können.

2. Gehen Sie nur dann wie folgt vor, wenn Sie es GuardDuty noch nicht aktiviert haben. Andernfalls können Sie diesen Schritt überspringen und mit dem nächsten Schritt fortfahren.

   Wenn Sie es noch nicht aktiviert haben GuardDuty, wählen Sie auf der GuardDuty Amazon-Seite Erste Schritte aus.

   Wählen Sie auf der Seite Welcome to (Willkommen bei) GuardDuty die Option Enable (Aktivieren) GuardDuty aus.

3. Gehen Sie nach der Aktivierung GuardDuty für Ihr Konto wie folgt vor, um die Einladung zur Mitgliedschaft anzunehmen:

   a. Wählen Sie im Navigationsbereich Settings (Einstellungen).

   b. Wählen Sie -Accounts (Konten).

   c. Stellen Sie sicher, dass Sie bei den Konten den Inhaber des Kontos verifizieren, von dem Sie die Einladung annehmen. Aktivieren Sie Annehmen, um die Einladung zur Mitgliedschaft anzunehmen.

4. Nachdem Sie die Einladung angenommen haben, wird Ihr Konto zu einem GuardDuty Mitgliedskonto. Das Konto, dessen Besitzer die Einladung gesendet hat, wird zum GuardDuty Administratorkonto. Das Administratorkonto wird wissen, dass Sie die Einladung angenommen haben. Die Kontentabelle in ihrem GuardDuty Konto wird aktualisiert.
   Der Wert in der Spalte Status, der Ihrer Mitgliedskonto-ID entspricht, wird auf Aktiviert geändert. Der Inhaber des Administratorkontos kann nun die Konfigurationen GuardDuty und Schutzpläne für Ihr Konto einsehen und verwalten. Das Administratorkonto kann auch die für Ihr Mitgliedskonto generierten GuardDuty Ergebnisse einsehen und verwalten.

API/CLI

Sie können über die API-Operationen ein GuardDuty Administratorkonto festlegen und GuardDuty Mitgliedskonten auf Einladung erstellen oder hinzufügen. Führen Sie die folgenden GuardDuty API-Operationen aus, um Administratorkonten und Mitgliedskonten in festzulegen. GuardDuty

Führen Sie das folgende Verfahren mit den Anmeldeinformationen des Kontos aus AWS-Konto , das Sie als GuardDuty Administratorkonto festlegen möchten.

Mitgliedskonten erstellen oder hinzufügen

1. Führen Sie den CreateMembersAPI-Vorgang mit den Anmeldeinformationen des AWS Kontos aus, das GuardDuty aktiviert wurde. Dies ist das Konto, das Sie als GuardDuty Administratorkonto verwenden möchten.

   Sie müssen die Melder-ID des AWS Girokontos sowie die Konto-ID und E-Mail-Adresse der Konten angeben, denen Sie GuardDuty beitreten möchten. Sie können mit dieser API-Operation ein oder mehrere Mitglieder erstellen.

   Sie können auch die AWS Befehlszeilentools verwenden, um ein Administratorkonto festzulegen, indem Sie den folgenden CLI-Befehl ausführen. Stellen Sie sicher, dass Sie Ihre eigene gültige Detektor-ID, Konto-ID und E-Mail verwenden.

   Um das `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, gehen Sie in der https://console.aws.amazon.com/guardduty/Konsole auf die Seite „Einstellungen“ oder führen Sie die ListDetectorsAPI aus.

   ```
   aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
   account-details AccountId=111122223333,Email=guardduty-member@organization.com
   ```

2. Verwenden Sie für die Ausführung InviteMembersdie Anmeldeinformationen des AWS Kontos, das GuardDuty aktiviert wurde. Dies ist das Konto, das Sie als GuardDuty Administratorkonto verwenden möchten.

   Sie müssen die Melder-ID des AWS Girokontos und die Konto-IDs der Konten angeben, denen Sie GuardDuty beitreten möchten. Sie können mit dieser API-Operation ein oder mehrere Mitglieder einladen.

   > **Note**
   >
   > Sie können mit dem `message`-Anfrageparameter auch eine optionale Einladungsbenachrichtigung erstellen.

Sie können sie auch verwenden AWS Command Line Interface , um Mitgliedskonten festzulegen, indem Sie den folgenden Befehl ausführen. Stellen Sie sicher, dass Sie Ihre eigene gültige Detektor-ID sowie gültige Konto-IDs für die Konten verwenden, die Sie einladen möchten.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

```
aws guardduty invite-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
account-ids 111122223333
```

Einladungen annehmen

Führen Sie das folgende Verfahren mit den Anmeldeinformationen jedes AWS Kontos aus, das Sie als GuardDuty Mitgliedskonto festlegen möchten.

1. Führen Sie den CreateDetectorAPI-Vorgang für jedes AWS Konto aus, das als GuardDuty Mitgliedskonto eingeladen wurde und das Sie annehmen möchten.

   Sie müssen angeben, ob die Detektorressource mithilfe des GuardDuty Dienstes aktiviert werden soll. Ein Detektor muss erstellt und aktiviert werden, damit er GuardDuty betriebsbereit ist. Sie müssen die Aktivierung zuerst aktivieren, GuardDuty bevor Sie eine Einladung annehmen können.

   Sie können dies auch mithilfe der AWS Befehlszeilentools mit dem folgenden CLI-Befehl tun.

   ```
   aws guardduty create-detector --enable
   ```

2. Führen Sie den AcceptAdministratorInvitationAPI-Vorgang für jedes AWS Konto aus, für das Sie die Einladung zur Mitgliedschaft annehmen möchten, und verwenden Sie dabei die Anmeldeinformationen dieses Kontos.

   Sie müssen die Melder-ID dieses AWS Kontos für das Mitgliedskonto, die Konto-ID des Administratorkontos, das die Einladung gesendet hat, und die Einladungs-ID der Einladung, die Sie annehmen, angeben. Die Konto-ID des Administratorkontos finden Sie in der Einladungs-E-Mail. Sie können sie auch mittels des API-Vorgangs ListInvitations ermitteln.

Sie können eine Einladung auch mit den AWS Befehlszeilentools annehmen, indem Sie den folgenden CLI-Befehl ausführen. Stellen Sie sicher, dass Sie eine gültige Detektor-ID, Administratorkonto-ID und Einladungs-ID verwenden.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

```
aws guardduty accept-invitation --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --administrator-id 444455556666 --invitation-
id 84b097800250d17d1872b34c4daadcf5
```

Konsolidierung von GuardDuty Administratorkonten unter einer einzigen Organisation

GuardDuty empfiehlt die Verwendung von Assoziation AWS Organizations bis zur Verwaltung von Mitgliedskonten unter einem delegierten GuardDuty Administratorkonto. Sie können das unten beschriebene Beispielverfahren verwenden, um das Administratorkonto und das per Einladung zugeordnete Mitglied in einer Organisation unter einem einzigen GuardDuty delegierten GuardDuty Administratorkonto zu konsolidieren.

> **Note**
>
> GuardDuty empfiehlt, Ihre Mitgliedskonten AWS Organizations anstelle von GuardDuty Einladungen zu verwalten. Weitere Informationen finden Sie unter Verwalten von Konten mit AWS Organizations.

Konten, die bereits von einem delegierten GuardDuty Administratorkonto verwaltet werden, oder aktive Mitgliedskonten, die einem delegierten GuardDuty Administratorkonto zugeordnet sind, können keinem anderen delegierten GuardDuty Administratorkonto hinzugefügt werden. Jede Organisation kann nur über ein delegiertes GuardDuty Administratorkonto pro Region verfügen, und jedes Mitgliedskonto kann nur über ein delegiertes Administratorkonto verfügen. GuardDuty

Wählen Sie eine bevorzugte Zugriffsmethode, um GuardDuty Administratorkonten unter einem einzigen delegierten GuardDuty Administratorkonto zu konsolidieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

   Verwenden Sie die Anmeldeinformationen des Verwaltungskontos der Organisation, um sich anzumelden.
2. Alle Konten, die Sie verwalten möchten, GuardDuty müssen Teil Ihrer Organisation sein. Informationen zum Hinzufügen eines Kontos zu Ihrer Organisation finden Sie unter Einen AWS-Konto einladen, Ihrer Organisation beizutreten.
3. Stellen Sie sicher, dass alle Mitgliedskonten dem Konto zugeordnet sind, das Sie als einziges delegiertes GuardDuty Administratorkonto festlegen möchten. Trennen Sie alle Mitgliedskonten, die noch mit den bereits vorhandenen Administratorkonten verknüpft sind.

   Die folgenden Schritte helfen Ihnen dabei, Mitgliedskonten vom bereits vorhandenen Administratorkonto zu trennen:

   a. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/
   b. Um sich anzumelden, verwenden Sie die Anmeldeinformationen des bereits vorhandenen Administratorkontos.
   c. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
   d. Wählen Sie auf der Seite Konten ein oder mehrere Konten aus, die Sie vom Administratorkonto trennen möchten.
   e. Wählen Sie Aktionen und dann Konto trennen.
   f. Wählen Sie Bestätigen, um den Schritt abzuschließen.
4. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Verwenden Sie die Anmeldeinformationen des Verwaltungskontos, um sich anzumelden.
5. Wählen Sie im Navigationsbereich Settings (Einstellungen). Geben Sie auf der Seite Einstellungen das delegierte GuardDuty Administratorkonto für die Organisation an.
6. Melden Sie sich mit dem angegebenen delegierten Administratorkonto an. GuardDuty
7. Fügen Sie Mitglieder der Organisation hinzu. Weitere Informationen finden Sie unter GuardDuty Konten verwalten mit AWS Organizations.

API/CLI

1. Alle Konten, die Sie verwalten möchten, GuardDuty müssen Teil Ihrer Organisation sein. Informationen zum Hinzufügen eines Kontos zu Ihrer Organisation finden Sie unter Einen AWS-Konto einladen, Ihrer Organisation beizutreten.
2. Stellen Sie sicher, dass alle Mitgliedskonten dem Konto zugeordnet sind, das Sie als einziges delegiertes GuardDuty Administratorkonto festlegen möchten.

   a. Führen Sie DisassociateMembersden Befehl aus, um die Zuordnung aller Mitgliedskonten aufzuheben, die noch mit den bereits vorhandenen Administratorkonten verknüpft sind.

   b. Alternativ können Sie den folgenden Befehl ausführen und ihn durch die Melder-ID des bereits vorhandenen Administratorkontos ersetzen, von dem Sie die Verknüpfung *777777777777* mit dem Mitgliedskonto trennen möchten. AWS Command Line Interface *666666666666*Ersetzen Sie es durch die AWS-Konto ID des Mitgliedskontos, dessen Verknüpfung Sie aufheben möchten.

   ```
   aws guardduty disassociate-members --detector-id 777777777777 --account-
   ids 666666666666
   ```

3. Führen Sie EnableOrganizationAdminAccountden Befehl aus, um ein AWS-Konto als delegiertes Administratorkonto zu delegieren. GuardDuty

   Alternativ können Sie den folgenden Befehl ausführen AWS Command Line Interface , um ein delegiertes Administratorkonto zu delegieren: GuardDuty

   ```
   aws guardduty enable-organization-admin-account --admin-account-id 777777777777
   ```

4. Fügen Sie Mitglieder der Organisation hinzu. Weitere Informationen finden Sie unter Create or add member member accounts using API.

> **Important**
>
> Um die Effektivität eines GuardDuty regionalen Dienstes zu maximieren, empfehlen wir Ihnen, Ihr delegiertes GuardDuty Administratorkonto festzulegen und alle Mitgliedskonten in jeder Region hinzuzufügen.

GuardDuty Überlegungen zum Exportieren von Mitgliedskontodaten im CSV-Format

Als GuardDuty Administratorkonto können Sie die Details des Mitgliedskontos im CSV-Format exportieren. Zu diesen Details gehören die ID des Mitgliedskontos, der Name, der Typ (durch AWS Organizations oder durch Einladung hinzugefügt) sowie der Konfigurationsstatus GuardDuty und die speziellen Schutzpläne.

Je nachdem, wie Sie die verschiedenen Mitgliedskonten verwalten, wird auf der Seite GuardDuty Konten die Option CSV exportieren angezeigt. Mithilfe der Option CSV exportieren können Sie ermitteln, für welche Mitgliedskonten ein bestimmter Schutzplan aktiviert ist.

Die folgende Liste enthält die Kriterien dafür, ob der CSV-Export auf Ihrer GuardDuty Kontoseite verfügbar sein wird oder nicht:

- Sie verwenden es nur AWS Organizations zur Verwaltung mehrerer Mitgliedskonten und die Gesamtzahl der Mitgliedskonten in Ihrer GuardDuty Organisation beträgt bis zu 5.000.
- Sie verwenden AWS Organizations sowohl die Einladungsmethode als auch die Einladungsmethode, und die Gesamtzahl der Mitgliedskonten in Ihrer GuardDuty Organisation beträgt bis zu 5.000.

  In diesem Szenario enthält die exportierte CSV-Datei, ob ein Mitgliedskonto über AWS Organizations oder mithilfe einer Einladungsmethode hinzugefügt wurde.
- Wenn Sie nur die auf Einladung basierende Methode zur Verwaltung mehrerer Mitgliedskonten verwenden, gibt es keine Option CSV exportieren.

GuardDuty Typen finden

Ein Befund ist eine Benachrichtigung, die GuardDuty generiert wird, wenn ein Hinweis auf eine verdächtige oder böswillige Aktivität in Ihrem AWS-Konto erkannt wird. GuardDuty generiert einen Befund in einem Konto, das aktiviert wurde GuardDuty.

Informationen zu wichtigen Änderungen an den GuardDuty Befundtypen, einschließlich neu hinzugefügter oder veralteter Findetypen, finden Sie unterDokumentenverlauf für Amazon GuardDuty.

Hinweise zu Erkenntnis-Typen, die nun außer Betrieb genommen wurden, finden Sie unter Nicht mehr aktive Erkenntnistypen.

GuardDuty EC2-Suchttypen

Die folgenden Erkenntnisse sind spezifisch für Amazon-EC2-Ressourcen und haben immer einen Ressourcentyp von `Instance`. Der Schweregrad und die Details der Erkenntnisse unterscheiden sich je nach Ressourcenrolle, die angibt, ob die EC2-Instance das Ziel verdächtiger Aktivitäten war oder der Akteur, der die Aktivitäten durchführte.

Die hier aufgeführten Erkenntnisse beinhalten die Datenquellen und Modelle, die zur Generierung dieses Erkenntnistyps verwendet wurden. Weitere Informationen zu Datenquellen und Modellen finden Sie unter GuardDuty grundlegende Datenquellen.

> **Hinweise**
>
> - Angaben zur EC2-Instance fehlen möglicherweise, wenn die Instance bereits beendet wurde oder wenn der zugrunde liegende API-Aufruf von einer EC2-Instance in einer anderen Region stammt.
> - EC2-Ergebnisse, die VPC-Flow-Logs als Datenquelle verwenden, unterstützen keinen IPv6-Verkehr.

Für alle EC2-Erkenntnisse wird empfohlen, die betreffende Ressource zu untersuchen, um festzustellen, ob sie sich erwartungsgemäß verhält. Wenn die Aktivität autorisiert ist, können Sie Unterdrückungsregeln oder Listen vertrauenswürdiger IP-Adressen verwenden, um Falschmeldungen für diese Ressource zu verhindern. Wenn die Aktivität unerwartet auftritt, besteht die bewährte Sicherheitsmethode darin, davon auszugehen, dass die Instance kompromittiert wurde, und die

unter Behebung einer potenziell kompromittierten Amazon EC2-Instance beschriebenen Aktionen auszuführen.

Themen

- Backdoor:EC2/C&CActivity.B
- Backdoor:EC2/C&CActivity.B!DNS
- Backdoor:EC2/DenialOfService.Dns
- Backdoor:EC2/DenialOfService.Tcp
- Backdoor:EC2/DenialOfService.Udp
- Backdoor:EC2/DenialOfService.UdpOnTcpPorts
- Backdoor:EC2/DenialOfService.UnusualProtocol
- Backdoor:EC2/Spambot
- Behavior:EC2/NetworkPortUnusual
- Behavior:EC2/TrafficVolumeUnusual
- CryptoCurrency:EC2/BitcoinTool.B
- CryptoCurrency:EC2/BitcoinTool.B!DNS
- DefenseEvasion:EC2/UnusualDNSResolver
- DefenseEvasion:EC2/UnusualDoHActivity
- DefenseEvasion:EC2/UnusualDoTActivity
- Impact:EC2/AbusedDomainRequest.Reputation
- Impact:EC2/BitcoinDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Custom
- Impact:EC2/PortSweep
- Impact:EC2/SuspiciousDomainRequest.Reputation
- Impact:EC2/WinRMBruteForce
- Recon:EC2/PortProbeEMRUnprotectedPort
- Recon:EC2/PortProbeUnprotectedPort
- Recon:EC2/Portscan
- Trojan:EC2/BlackholeTraffic
- Trojan:EC2/BlackholeTraffic!DNS

- Trojan:EC2/DGADomainRequest.B
- Trojan:EC2/DGADomainRequest.C!DNS
- Trojan:EC2/DNSDataExfiltration
- Trojan:EC2/DriveBySourceTraffic!DNS
- Trojan:EC2/DropPoint
- Trojan:EC2/DropPoint!DNS
- Trojan:EC2/PhishingDomainRequest!DNS
- UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
- UnauthorizedAccess:EC2/MetadataDNSRebind
- UnauthorizedAccess:EC2/RDPBruteForce
- UnauthorizedAccess:EC2/SSHBruteForce
- UnauthorizedAccess:EC2/TorClient
- UnauthorizedAccess:EC2/TorRelay

Backdoor:EC2/C&CActivity.B

Eine EC2-Instance fragt eine IP-Adresse ab, die einem bekannten Command-and-Control-Server zugeordnet wird.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte Instance in Ihrer AWS -Umgebung eine IP-Adresse abfragt, der einem bekannten Command-and-Control (C&C)-Server zugeordnet ist. Die aufgeführte Instance ist möglicherweise kompromittiert. Command-and-control-Server sind Computer, die Befehle an Mitglieder eines Botnets senden.

Ein Botnet ist eine Sammlung von mit dem Internet verbundenen Geräten, zu denen PCs, Server, mobile Geräte und Geräte des Internets der Dinge gehören können, die mit einem allgemeinen Typ von Malware infiziert sind und von dieser kontrolliert werden. Botnets dienen häufig zum Verteilen von Malware und zum Sammeln von sich widerrechtlich angeeigneten Informationen, wie z. B. Kreditkartennummern. Je nach Zweck und Struktur des Botnets kann der C&C-Server auch den Befehl erteilen, einen Distributed Denial of Service (DDoS)-Angriff zu starten.

> **Note**
>
> Wenn die abgefragte IP log4j-bezogen ist, enthalten die Felder der zugehörigen Erkenntnis die folgenden Werte:
>
> - service.additional = Amazon Info.threatListName
> - service.additional = Log4j Verwandt Info.threatName

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Backdoor:EC2/C&CActivity.B!DNS

Eine EC2-Instance fragt einen Domainnamen ab, der einem bekannten Command-and-Control-Server zugeordnet wird.

Standard-Schweregrad: Hoch

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte Instance in Ihrer AWS -Umgebung einen Domainnamen abfragt, der einem bekannten Command-and-Control (C&C)-Server zugeordnet ist. Die aufgeführte Instance ist möglicherweise kompromittiert. Command-and-control-Server sind Computer, die Befehle an Mitglieder eines Botnets senden.

Ein Botnet ist eine Sammlung von mit dem Internet verbundenen Geräten, zu denen PCs, Server, mobile Geräte und Geräte des Internets der Dinge gehören können, die mit einem allgemeinen Typ von Malware infiziert sind und von dieser kontrolliert werden. Botnets dienen häufig zum Verteilen von Malware und zum Sammeln von sich widerrechtlich angeeigneten Informationen, wie z. B. Kreditkartennummern. Je nach Zweck und Struktur des Botnets kann der C&C-Server auch den Befehl erteilen, einen Distributed Denial of Service (DDoS)-Angriff zu starten.

> **Note**
>
> Wenn der abgefragte Domainname mit log4j zu tun hat, enthalten die Felder der zugehörigen Erkenntnis die folgenden Werte:

- service.additional = Amazon Info.threatListName
- service.additional = Log4j Verwandt Info.threatName

> **Note**
>
> Um zu testen, wie dieser Suchtyp GuardDuty generiert wird, können Sie von Ihrer Instance aus eine DNS-Anfrage (`dig`für Linux oder `nslookup` Windows) für eine Testdomäne stellen. `guarddutyc2activityb.com`

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Backdoor:EC2/DenialOfService.Dns

Das Verhalten einer EC2-Instance weist darauf hin, dass sie möglicherweise gerade für die Ausführung eines Denial-of-Service (DoS)-Angriffs mithilfe des DNS-Protokolls genutzt wird.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Dieses Ergebnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS -Umgebung eine große Menge ausgehenden DNS-Datenverkehrs generiert. Dies kann ein Hinweis darauf sein, dass die aufgeführte Instance kompromittiert wurde und mithilfe des DNS-Protokolls gerade für die Ausführung von Denial-of-Service (DoS)-Angriffen genutzt wird.

> **Note**
>
> Diese Erkenntnis erkennt nur DoS-Angriffe auf öffentlich routingfähige IP-Adressen, die das primäre Ziel von DoS-Angriffen sind.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Backdoor:EC2/DenialOfService.Tcp

Das Verhalten einer EC2-Instance weist darauf hin, dass sie möglicherweise gerade für die Ausführung eines Denial-of-Service (DoS)-Angriffs mithilfe des TCP-Protokolls genutzt wird.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS -Umgebung eine große Menge ausgehenden TCP-Datenverkehrs generiert. Dies kann ein Hinweis darauf sein, dass die Instance kompromittiert wurde und mithilfe des TCP-Protokolls gerade für die Ausführung von Denial-of-Service (DoS)-Angriffen genutzt wird.

> **Note**
>
> Diese Erkenntnis erkennt nur DoS-Angriffe auf öffentlich routingfähige IP-Adressen, die das primäre Ziel von DoS-Angriffen sind.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Backdoor:EC2/DenialOfService.Udp

Das Verhalten einer EC2-Instance weist darauf hin, dass sie möglicherweise gerade für die Ausführung eines Denial-of-Service (DoS)-Angriffs mithilfe des UDP-Protokolls genutzt wird.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS -Umgebung eine große Menge ausgehenden UDP-Datenverkehrs generiert. Dies kann ein Hinweis darauf sein, dass die aufgeführte Instance kompromittiert wurde und mithilfe des UDP-Protokolls gerade für die Ausführung von Denial-of-Service (DoS)-Angriffen genutzt wird.

> **Note**
>
> Diese Erkenntnis erkennt nur DoS-Angriffe auf öffentlich routingfähige IP-Adressen, die das primäre Ziel von DoS-Angriffen sind.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Backdoor:EC2/DenialOfService.UdpOnTcpPorts

Das Verhalten einer EC2-Instance weist darauf hin, dass sie möglicherweise gerade für die Ausführung eines Denial-of-Service (DoS)-Angriffs mithilfe des UDP-Protokolls auf einem TCP-Port genutzt wird.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie, dass die aufgeführte EC2-Instance in Ihrer AWS -Umgebung eine große Menge ausgehenden UDP-Datenverkehrs generiert, der auf einen Port zielt, der normalerweise für die TCP-Kommunikation verwendet wird. Dies kann ein Hinweis darauf sein, dass die aufgeführte Instance kompromittiert wurde und mithilfe des UDP-Protokolls auf einem TCP-Port gerade für die Ausführung von Denial-of-Service (DoS)-Angriffen genutzt wird.

> **Note**
>
> Diese Erkenntnis erkennt nur DoS-Angriffe auf öffentlich routingfähige IP-Adressen, die das primäre Ziel von DoS-Angriffen sind.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Backdoor:EC2/DenialOfService.UnusualProtocol

Das Verhalten einer EC2-Instance weist darauf hin, dass sie möglicherweise gerade für die Ausführung eines Denial-of-Service (DoS)-Angriffs mithilfe eines ungewöhnlichen Protokolls genutzt wird.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie, dass die aufgeführte EC2-Instance in Ihrer AWS -Umgebung eine große Menge ausgehenden Datenverkehrs eines ungewöhnlichen Protokolltyps generiert, der normalerweise nicht von EC2-Instances verwendet wird (beispielsweise ein Internet Group Management Protocol). Dies kann ein Hinweis darauf sein, dass die Instance kompromittiert wurde und mithilfe eines ungewöhnlichen Protokolls gerade für die Ausführung von Denial-of-Service (DoS)-Angriffen genutzt wird. Diese Erkenntnis erkennt nur DoS-Angriffe auf öffentlich routingfähige IP-Adressen, die das primäre Ziel von DoS-Angriffen sind.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Backdoor:EC2/Spambot

Eine EC2-Instance zeigt ungewöhnliches Verhalten, indem sie mit einem Remote-Host auf Port 25 kommuniziert.

Standard-Schweregrad: Mittel

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS -Umgebung mit einem Remote-Host auf Port 25 kommuniziert. Dieses Verhalten ist ungewöhnlich, da die

betreffende EC2-Instance zuvor nicht über Port 25 kommuniziert hat. Port 25 wird in der Regel von Mailservern für die SMTP-Kommunikation verwendet. Diese Erkenntnis weist darauf hin, dass Ihre EC2-Instance möglicherweise kompromittiert ist und für das Versenden von Spam eingesetzt wird.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Behavior:EC2/NetworkPortUnusual

Eine EC2-Instance kommuniziert auf einem unüblichen Serverport mit einem Remote-Host.

Standard-Schweregrad: Mittel

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS -Umgebung ein Verhalten zeigt, das von ihrem normalen Verhalten abweicht. Diese EC2-Instance hat zuvor nicht auf diesem Remote-Port kommuniziert.

> **Note**
>
> Wenn die EC2-Instance über Port 389 oder Port 1389 kommuniziert hat, wird der zugehörige Erkenntnis-Schweregrad auf Hoch geändert, und die Erkenntnisfelder enthalten den folgenden Wert:
>
> - service.additional Info.context = Möglicher log4j-Callback

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Behavior:EC2/TrafficVolumeUnusual

Eine EC2-Instance generiert ungewöhnlich große Mengen an Netzwerkdatenverkehr zu einem Remote-Host.

Standard-Schweregrad: Mittel

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS -Umgebung ein Verhalten zeigt, das von ihrem normalen Verhalten abweicht. Diese EC2-Instance hat bisher keine derartig hohe Menge an Datenverkehr an diesen Remote-Host gesendet.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

CryptoCurrency:EC2/BitcoinTool.B

Eine EC2-Instance fragt eine IP-Adresse ab, die mit einer Aktivität in Zusammenhang mit einer Kryptowährung steht.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS -Umgebung eine IP-Adresse abfragt, die mit einer Aktivität in Zusammenhang mit Bitcoin oder einer anderen Kryptowährung in Verbindung steht. Bitcoin ist ein weltweites Kryptowährungs- und digitales Zahlungssystem, das gegen andere Währungen, Produkte und Services eingetauscht werden kann. Bitcoin ist eine Belohnung für das Bitcoin-Mining und bei Bedrohungsakteuren sehr gefragt.

Empfehlungen zur Abhilfe:

Wenn Sie diese EC2-Instance verwenden, um Kryptowährung zu minen oder zu verwalten, oder diese Instance anderweitig an der Blockchain-Aktivität beteiligt ist, könnte diese Erkenntnis erwartete Aktivitäten für Ihre Umgebung repräsentieren. Wenn dies in Ihrer AWS -Umgebung der Fall ist,

empfehlen wir, für diese Erkenntnis eine Unterdrückungsregel festzulegen. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Ergebnistyp mit dem Wert `CryptoCurrency:EC2/BitcoinTool.B` verwenden. Das zweite Filterkriterium sollte die Instance-ID der Instance sein, die an der Blockchain-Aktivität beteiligt ist. Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln in GuardDuty.

Wenn diese Aktivität unerwartet ist, ist Ihre Instance wahrscheinlich kompromittiert. Informationen dazu finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

CryptoCurrency:EC2/BitcoinTool.B!DNS

Eine EC2-Instance fragt einen Domainnamen ab, der mit einer Aktivität in Zusammenhang mit einer Kryptowährung steht.

Standard-Schweregrad: Hoch

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS -Umgebung einen Domainnamen abfragt, die mit einer Aktivität in Zusammenhang mit Bitcoin oder einer anderen Kryptowährung in Verbindung steht. Bitcoin ist ein weltweites Kryptowährungs- und digitales Zahlungssystem, das gegen andere Währungen, Produkte und Services eingetauscht werden kann. Bitcoin ist eine Belohnung für das Bitcoin-Mining und bei Bedrohungsakteuren sehr gefragt.

Empfehlungen zur Abhilfe:

Wenn Sie diese EC2-Instance verwenden, um Kryptowährung zu minen oder zu verwalten, oder diese Instance anderweitig an der Blockchain-Aktivität beteiligt ist, könnte diese Erkenntnis erwartete Aktivitäten für Ihre Umgebung repräsentieren. Wenn dies in Ihrer AWS -Umgebung der Fall ist, empfehlen wir, für diese Erkenntnis eine Unterdrückungsregel festzulegen. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Ergebnistyp mit dem Wert `CryptoCurrency:EC2/BitcoinTool.B!DNS` verwenden. Das zweite Filterkriterium sollte die Instance-ID der Instance sein, die an der Blockchain-Aktivität beteiligt ist. Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln in GuardDuty.

Wenn diese Aktivität unerwartet ist, ist Ihre Instance wahrscheinlich kompromittiert. Informationen dazu finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

DefenseEvasion:EC2/UnusualDNSResolver

Eine Amazon-EC2-Instance kommuniziert mit einem ungewöhnlichen öffentlichen DNS-Resolver.

Standard-Schweregrad: Mittel

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte Amazon-EC2-Instance in Ihrer AWS -Umgebung ein Verhalten zeigt, das von ihrem normalen Verhalten abweicht. Diese EC2-Instance hat in letzter Zeit nicht mit diesem öffentlichen DNS-Resolver kommuniziert. Das Feld Ungewöhnlich im Bereich mit den Suchdetails in der GuardDuty Konsole kann Informationen über den abgefragten DNS-Resolver enthalten.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

DefenseEvasion:EC2/UnusualDoHActivity

Eine Amazon-EC2-Instance führt eine ungewöhnliche DNS-über-HTTPS-Kommunikation (DoH) durch.

Standard-Schweregrad: Mittel

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte Amazon-EC2-Instance in Ihrer AWS -Umgebung ein Verhalten zeigt, das von ihrem normalen Verhalten abweicht. Diese EC2-Instance hat in letzter Zeit keine DNS-über-HTTPS-Kommunikation (DoH) mit diesem öffentlichen DoH-Server durchgeführt. Das Feld Ungewöhnlich in den Erkenntnisdetails kann Informationen über den abgefragten DoH-Server enthalten.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

DefenseEvasion:EC2/UnusualDoTActivity

Eine Amazon-EC2-Instance führt eine ungewöhnliche DNS-über-TLS-Kommunikation (DoT) durch.

Standard-Schweregrad: Mittel

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS -Umgebung ein Verhalten zeigt, das von ihrem normalen Verhalten abweicht. Diese EC2-Instance hat in letzter Zeit keine DNS-über-TLS-Kommunikation (DoT) mit diesem öffentlichen DoT-Server durchgeführt. Das Feld Ungewöhnlich in den Erkenntnisdetails kann Informationen über den abgefragten DoT-Server enthalten.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Impact:EC2/AbusedDomainRequest.Reputation

Eine EC2-Instance fragt einen Domainnamen mit geringer Reputation ab, der mit bekanntermaßen missbrauchten Domains in Verbindung steht.

Standard-Schweregrad: Mittel

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte Amazon-EC2-Instance in Ihrer AWS -Umgebung einen Domainnamen mit niedriger Reputation abfragt, der mit bekannten missbrauchten Domains oder IP-Adressen in Verbindung steht. Beispiele für missbrauchte Domains sind Top-Level-Domainnamen (TLDs) und Second-Level-Domainnamen (2LDs), die kostenlose Subdomain-Registrierungen bieten, sowie dynamische DNS-Anbieter. Bedrohungsakteure nutzen diese Services in der Regel, um Domains kostenlos oder zu geringen Kosten zu registrieren. Bei Domains mit geringer Reputation in dieser Kategorie kann es sich auch um abgelaufene Domains handeln, die auf die Parking-IP-Adresse eines Registrars zurückgehen und daher möglicherweise nicht mehr aktiv sind. Bei einer Parking-IP leitet ein Registrar den Verkehr für Domains weiter, die mit keinem

Service verknüpft wurden. Die aufgeführte Amazon-EC2-Instance kann kompromittiert sein, da Bedrohungsakteure diese Registrare oder Services häufig für C&C und die Verbreitung von Malware nutzen.

Domains mit niedriger Reputation basieren auf einem Reputations-Punkte-Modell. Dieses Modell bewertet und bewertet die Eigenschaften einer Domain, um zu ermitteln, ob es sich um eine bösartige Domain handeln könnte.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Impact:EC2/BitcoinDomainRequest.Reputation

Eine EC2-Instance fragt einen Domainnamen ab, der mit einer Aktivität in Zusammenhang mit einer Kryptowährung steht.

Standard-Schweregrad: Hoch

- Datenquelle: DNS-Protokolle

Dieses Ergebnis informiert Sie, dass die aufgeführte Amazon-EC2-Instance in Ihrer AWS -Umgebung einen Domainnamen mit niedriger Reputation abfragt, der mit einer Aktivität in Zusammenhang mit Bitcoin oder einer anderen Kryptowährung in Verbindung steht. Bitcoin ist ein weltweites Kryptowährungs- und digitales Zahlungssystem, das gegen andere Währungen, Produkte und Services eingetauscht werden kann. Bitcoin ist eine Belohnung für das Bitcoin-Mining und bei Bedrohungsakteuren sehr gefragt.

Domains mit niedriger Reputation basieren auf einem Reputations-Punkte-Modell. Dieses Modell bewertet und bewertet die Eigenschaften einer Domain, um zu ermitteln, ob es sich um eine bösartige Domain handeln könnte.

Empfehlungen zur Abhilfe:

Wenn Sie diese EC2-Instance verwenden, um Kryptowährung zu minen oder zu verwalten, oder diese Instance anderweitig an der Blockchain-Aktivität beteiligt ist, könnte diese Erkenntnis erwartete Aktivitäten für Ihre Umgebung repräsentieren. Wenn dies in Ihrer AWS -Umgebung der Fall ist, empfehlen wir, für diese Erkenntnis eine Unterdrückungsregel festzulegen. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Ergebnistyp mit dem

Wert `Impact:EC2/BitcoinDomainRequest.Reputation` verwenden. Das zweite Filterkriterium sollte die Instance-ID der Instance sein, die an der Blockchain-Aktivität beteiligt ist. Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln in GuardDuty.

Wenn diese Aktivität unerwartet ist, ist Ihre Instance wahrscheinlich kompromittiert. Informationen dazu finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Impact:EC2/MaliciousDomainRequest.Reputation

Eine EC2-Instance fragt eine Domain mit niedriger Reputation ab, die mit bekannten bösartigen Domains in Verbindung stehen.

Standard-Schweregrad: Hoch

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte Amazon-EC2-Instance in Ihrer AWS -Umgebung einen Domainnamen mit niedriger Reputation abfragt, der mit bekannten bösartigen Domains oder IP-Adressen in Verbindung stehen. Beispielsweise können Domains mit einer bekannten Sinkhole-IP-Adresse verknüpft sein. Sinkhole-Domains sind Domains, die zuvor von einem Bedrohungsakteur kontrolliert wurden, und Anfragen an sie können darauf hinweisen, dass die Instance kompromittiert wurde. Diese Domains können auch mit bekannten böswilligen Kampagnen oder Algorithmen zur Domain-Generierung korreliert sein.

Domains mit niedriger Reputation basieren auf einem Reputations-Punkte-Modell. Dieses Modell bewertet und bewertet die Eigenschaften einer Domain, um zu ermitteln, ob es sich um eine bösartige Domain handeln könnte.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Impact:EC2/MaliciousDomainRequest.Custom

Eine EC2-Instance fragt eine Domain auf einer benutzerdefinierten Liste von Bedrohungsentitäten ab.

Standard-Schweregrad: Mittel

- Datenquelle: DNS-Protokolle

Dieses Ergebnis informiert Sie darüber, dass die aufgelistete Amazon EC2 EC2-Instance in Ihrer AWS Umgebung einen Domainnamen abfragt, der in der Liste der Bedrohungsentitäten enthalten ist, die Sie hochgeladen und aktiviert haben. In GuardDuty besteht eine Liste von Bedrohungsinstanzen aus bekannten bösartigen Domainnamen und IP-Adressen. GuardDuty generiert Ergebnisse auf der Grundlage der Aktivitäten, die mit der hochgeladenen Liste der bedrohlichen Entitäten verknüpft sind. Den Namen der Liste der bedrohlichen Entitäten finden Sie in den Ergebnisdetails.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Impact:EC2/PortSweep

Eine EC2-Instance untersucht einen Port auf einer großen Anzahl von IP-Adressen.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Dieses Ergebnis informiert Sie darüber, dass die aufgelistete EC2-Instance in Ihrer AWS Umgebung einen Port auf einer großen Anzahl von öffentlich routbaren IP-Adressen untersucht. Diese Art von Aktivität wird in der Regel verwendet, um anfällige Hosts zu finden, die ausgenutzt werden können. Im Bereich mit den Ergebnisdetails in Ihrer GuardDuty Konsole wird nur die neueste Remote-IP-Adresse angezeigt

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Impact:EC2/SuspiciousDomainRequest.Reputation

Eine EC2-Instance fragt einen Domainnamen mit geringer Reputation ab, der aufgrund seines Alters oder seiner geringen Beliebtheit verdächtig ist.

Standard-Schweregrad: Niedrig

- Datenquelle: DNS-Protokolle

Dieses Ergebnis informiert Sie darüber, dass die aufgeführte Amazon-EC2-Instance in Ihrer AWS -Umgebung einen Domainnamen mit niedriger Reputation abfragt, bei dem der Verdacht besteht, dass er bösartig ist. Es wurden Merkmale dieser Domain festgestellt, die mit zuvor beobachteten bösartigen Domains übereinstimmten. Unser Reputationsmodell konnte sie jedoch nicht definitiv mit einer bekannten Bedrohung in Verbindung bringen. Diese Domains werden in der Regel neu beobachtet oder erhalten nur wenig Datenverkehr.

Domains mit niedriger Reputation basieren auf einem Reputations-Punkte-Modell. Dieses Modell bewertet und bewertet die Eigenschaften einer Domain, um zu ermitteln, ob es sich um eine bösartige Domain handeln könnte.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Impact:EC2/WinRMBruteForce

Eine EC2-Instance führt einen ausgehenden Brute-Force-Angriff für die Windows-Remoteverwaltung durch.

Standard-Schweregrad: Niedrig*

> **Note**
>
> Der Schweregrad dieser Erkenntnis ist niedrig, wenn Ihre EC2-Instance das Ziel eines Brute-Force-Angriffs war. Der Schweregrad dieser Erkenntnis ist hoch, wenn Ihre EC2-Instance der zum Ausführen eines Brute-Force-Angriffs verwendete Akteur ist.

- Datenquelle: VPC-Flow-Protokolle

Dieses Ergebnis informiert Sie darüber, dass die aufgelistete EC2-Instance in Ihrer AWS Umgebung einen Brute-Force-Angriff (Windows Remote Management, WinRM) ausführt, der darauf abzielt, Zugriff auf den Windows-Fernverwaltungsdienst auf Systemen zu erhalten. Windows-based

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Recon:EC2/PortProbeEMRUnprotectedPort

Eine EC2-Instance verfügt über einen ungeschützten EMR-bezogenen Port, der von einem bekannten böswilligen Host untersucht wird.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Dieses Ergebnis informiert Sie darüber, dass ein EMR-bezogener sensibler Port auf der aufgelisteten EC2-Instance, die Teil eines Clusters in Ihrer AWS Umgebung ist, nicht durch eine Sicherheitsgruppe, eine Zugriffskontrollliste (ACL) oder eine On-Host-Firewall wie Linux IPTables blockiert wird. Dieses Ergebnis gibt auch Aufschluss darüber, dass bekannte Scanner im Internet diesen Port aktiv untersuchen. Ports, die diese Erkenntnis auslösen können, z. B. Port 8088 (YARN Web-UI-Port), könnten potenziell für die Remote-Code-Ausführung genutzt werden.

Empfehlungen zur Abhilfe:

Sie sollten den offenen Zugang zu Ports auf Clustern aus dem Internet blockieren und den Zugang nur auf bestimmte IP-Adressen beschränken, die Zugang zu diesen Ports benötigen. Weitere Informationen finden Sie unter Sicherheitsgruppen für EMR-Cluster.

Recon:EC2/PortProbeUnprotectedPort

Eine EC2-Instance hat einen ungeschützten Port, der von einem bekannten böswilligen Host getestet wird.

Standard-Schweregrad: Niedrig*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Niedrig. Wenn der Port, der untersucht wird, jedoch von Elasticsearch (9200 oder 9300) verwendet wird, ist der Schweregrad des Ergebnisses hoch.

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie, dass ein Port auf der aufgeführten EC2-Instance in Ihrer AWS -Umgebung nicht durch eine Sicherheitsgruppe, eine Zugriffssteuerungsliste (ACL) oder eine On-Host-Firewall wie Linux IPTables blockiert ist und derzeit aktiv von bekannten Scannern im Internet untersucht wird.

Wenn der identifizierte ungeschützte Port 22 oder 3389 ist und Sie sich über diese Ports mit Ihrer Instance verbinden, können Sie die Exposition dennoch einschränken, indem Sie den Zugriff auf diese Ports nur für die IP-Adressen aus dem IP-Adressraum Ihres Unternehmensnetzwerks zulassen. Informationen zum Einschränken des Zugriffs auf Port 22 unter Linux finden Sie unter Autorisieren von eingehendem Datenverkehr für Linux-Instances. Informationen zum Einschränken des Zugriffs auf Port 3389 unter Windows finden Sie unter Autorisieren von eingehendem Datenverkehr für Windows-Instances.

GuardDuty generiert diesen Befund nicht für die Ports 443 und 80.

Empfehlungen zur Abhilfe:

In einigen Fällen werden Instances absichtlich exponiert, weil sie beispielsweise Webserver hosten. Wenn dies in Ihrer AWS Umgebung der Fall ist, empfehlen wir Ihnen, eine Unterdrückungsregel für dieses Ergebnis einzurichten. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Ergebnistyp mit dem Wert `Recon:EC2/PortProbeUnprotectedPort` verwenden. Das zweite Filterkriterium sollte der oder den Instances entsprechen, die als Bastion-Host eingesetzt werden. Sie können entweder das Attribut Instance-Image-ID oder das Attribut Tag verwenden, abhängig davon, welches Kriterium mit den Instances identifiziert werden kann, die diese Tools hosten. Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln in GuardDuty.

Wenn diese Aktivität unerwartet ist, ist Ihre Instance wahrscheinlich kompromittiert. Informationen dazu finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Recon:EC2/Portscan

Eine EC2-Instance führt ausgehende Port-Scans an einem Remote-Host durch.

Standard-Schweregrad: Mittel

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie, dass die aufgeführte EC2-Instance in Ihrer AWS -Umgebung an einem möglichen Port-Scan-Angriff beteiligt ist, da sie versucht, in kurzer Zeit Verbindungen zu mehreren Ports herzustellen. Das Ziel eines Port-Scan-Angriffs ist die Ermittlung offener Ports, um zu ermitteln, welche Services und welches Betriebssystem der Computer ausführt.

Empfehlungen zur Abhilfe:

Diese Erkenntnis kann falsch positiv sein, wenn Anwendungen zur Schwachstellenbewertung auf EC2-Instances in der Umgebung bereitgestellt werden, weil diese Anwendungen Port-Scans durchführen, um Sie über falsch konfigurierte offene Ports zu informieren. Wenn dies in Ihrer AWS Umgebung der Fall ist, empfehlen wir Ihnen, eine Unterdrückungsregel für dieses Ergebnis einzurichten. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Ergebnistyp mit dem Wert `Recon:EC2/Portscan` verwenden. Das zweite Filterkriterium sollte den Instances entsprechen, die diese Tools zur Schwachstellenanalyse hosten. Sie können entweder das Attribut Instance-Image-ID oder das Attribut Tag verwenden, abhängig davon, welches Kriterium mit den Instances identifiziert werden kann, die diese Tools hosten. Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln in GuardDuty.

Wenn diese Aktivität unerwartet ist, ist Ihre Instance wahrscheinlich kompromittiert. Informationen dazu finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Trojan:EC2/BlackholeTraffic

Eine EC2-Instance versucht, mit einer IP-Adresse eines Remote-Hosts zu kommunizieren, der ein bekanntes schwarzes Loch ist.

Standard-Schweregrad: Mittel

- Datenquelle: VPC-Flow-Protokolle

Dieses Ergebnis informiert Sie darüber, dass die aufgelistete EC2-Instance in Ihrer AWS Umgebung möglicherweise gefährdet ist, weil sie versucht, mit der IP-Adresse eines schwarzen Lochs (oder Sink Hole) zu kommunizieren. Schwarze Löcher sind Stellen im Netzwerk, an denen ein- oder ausgehender Datenverkehr unbemerkt verworfen wird, ohne dass die Quelle darüber informiert wird, dass die Daten den vorgesehenen Empfänger nicht erreicht haben. Die IP-Adresse eines schwarzen Lochs gibt einen Hostcomputer an, der nicht ausgeführt wird, oder eine Adresse, der kein Host zugewiesen wurde.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Trojan:EC2/BlackholeTraffic!DNS

Eine EC2-Instance fragt einen Domainnamen ab, der an eine die IP-Adresse eines schwarzen Lochs weitergeleitet wird.

Standard-Schweregrad: Mittel

- Datenquelle: DNS-Protokolle

Dieses Ergebnis informiert Sie darüber, dass die aufgelistete EC2-Instance in Ihrer AWS Umgebung möglicherweise gefährdet ist, weil sie einen Domainnamen abfragt, der an eine Black-Hole-IP-Adresse umgeleitet wird. Schwarze Löcher sind Stellen im Netzwerk, an denen ein- oder ausgehender Datenverkehr unbemerkt verworfen wird, ohne dass die Quelle darüber informiert wird, dass die Daten den vorgesehenen Empfänger nicht erreicht haben.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Trojan:EC2/DGADomainRequest.B

Eine EC2-Instance fragt algorithmisch generierte Domänen ab. Solche Domänen werden häufig von Malware genutzt und können auf eine kompromittierte EC2-Instance hinweisen.

Standard-Schweregrad: Hoch

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS -Umgebung versucht, DGA (Domain Generation Algorithms)-Domains abzufragen. Ihre EC2-Instance wurde möglicherweise kompromittiert.

DGAs werden verwendet, um in regelmäßigen Abständen eine große Anzahl an Domainnamen zu generieren, die als Rendezvous Points mit ihren Command-and-Control (C&C)-Servern verwendet werden können. Command-and-Control-Server sind Computer, die Befehle an die Mitglieder eines Botnets senden. Hierbei handelt es sich um eine Ansammlung von mit dem Internet verbundenen Geräten, die infiziert sind und von einer gängigen Malware kontrolliert werden. Die große Anzahl potenzieller Rendezvous Points erschwert ein effektives Stilllegen von Botnets, da infizierte Computer versuchen, einige dieser Domainnamen täglich zu kontaktieren, um Updates oder Befehle zu erhalten.

> **Note**
>
> Diese Erkenntnis basiert auf der Analyse von Domainnamen mit erweiterten Heuristiken und kann daher neue DGA-Domains identifizieren, die nicht in Bedrohungsdaten-Feeds vorhanden sind.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Trojan:EC2/DGADomainRequest.C!DNS

Eine EC2-Instance fragt algorithmisch generierte Domänen ab. Solche Domänen werden häufig von Malware genutzt und können auf eine kompromittierte EC2-Instance hinweisen.

Standard-Schweregrad: Hoch

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS -Umgebung versucht, DGA (Domain Generation Algorithms)-Domains abzufragen. Ihre EC2-Instance wurde möglicherweise kompromittiert.

DGAs werden verwendet, um in regelmäßigen Abständen eine große Anzahl an Domainnamen zu generieren, die als Rendezvous Points mit ihren Command-and-Control (C&C)-Servern verwendet werden können. Command-and-Control-Server sind Computer, die Befehle an die Mitglieder eines

Botnets senden. Hierbei handelt es sich um eine Ansammlung von mit dem Internet verbundenen Geräten, die infiziert sind und von einer gängigen Malware kontrolliert werden. Die große Anzahl potenzieller Rendezvous Points erschwert ein effektives Stilllegen von Botnets, da infizierte Computer versuchen, einige dieser Domainnamen täglich zu kontaktieren, um Updates oder Befehle zu erhalten.

> **Note**
>
> Dieses Ergebnis basiert auf bekannten DGA-Domänen aus GuardDuty den Threat-Intelligence-Feeds.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Trojan:EC2/DNSDataExfiltration

Eine EC2-Instance filtert Daten durch DNS-Abfragen heraus.

Standard-Schweregrad: Hoch

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS -Umgebung Malware ausführt, die DNS-Abfragen für ausgehende Datenübertragungen verwendet. Diese Art der Datenübertragung weist auf eine kompromittierte Instance hin und kann zur Exfiltration von Daten führen. DNS-Datenverkehr wird in der Regel nicht durch Firewalls gesperrt. So kann beispielsweise Malware in einer kompromittierten EC2-Instance Daten verschlüsseln (z. B. Ihre Kreditkartennummer) und in einer DNS-Abfrage an einen entfernten DNS-Server senden, der von einem Angreifer gesteuert wird.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Trojan:EC2/DriveBySourceTraffic!DNS

Eine EC2-Instance fragt den Domainnamen eines Remote-Hosts ab, der eine bekannte Quelle für Download-Angriffe ist. Drive-By

Standard-Schweregrad: Hoch

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie, dass die aufgeführte EC2-Instance in Ihrer AWS -Umgebung möglicherweise kompromittiert wurde, da Sie einen Domainnamen von einem Remote-Host abfragt, der eine bekannte Quelle von Drive-By-Download-Angriffen ist. Hierbei handelt es sich um unbeabsichtigte Downloads von Computersoftware aus dem Internet, die eine automatische Installation von Viren, Spyware oder Malware auslösen kann.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Trojan:EC2/DropPoint

Eine EC2-Instance versucht, mit einer IP-Adresse eines Remote-Hosts zu kommunizieren, von dem bekannt ist, dass er Anmeldedaten und andere mithilfe von Malware gestohlene Daten enthält.

Standard-Schweregrad: Mittel

- Datenquelle: VPC-Flow-Protokolle

Dieses Ergebnis informiert Sie darüber, dass eine EC2-Instance in Ihrer AWS Umgebung versucht, mit der IP-Adresse eines Remote-Hosts zu kommunizieren, auf dem sich bekanntermaßen Anmeldeinformationen und andere gestohlene Daten befinden, die von Malware erfasst wurden.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Trojan:EC2/DropPoint!DNS

Eine EC2-Instance fragt einen Domainnamen eines Remote-Hosts ab, von dem bekannt ist, dass er Anmeldedaten und andere mithilfe von Malware gestohlene Daten enthält.

Standard-Schweregrad: Mittel

- Datenquelle: DNS-Protokolle

Dieses Ergebnis informiert Sie darüber, dass eine EC2-Instance in Ihrer AWS Umgebung den Domainnamen eines Remote-Hosts abfragt, der bekanntermaßen Anmeldeinformationen und andere gestohlene Daten enthält, die von Malware erfasst wurden.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Trojan:EC2/PhishingDomainRequest!DNS

Eine EC2-Instance fragt Domänen ab, die an Phishing-Angriffen beteiligt sind. Ihre EC2-Instance wurde möglicherweise kompromittiert.

Standard-Schweregrad: Hoch

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie darüber, dass eine EC2-Instance in Ihrer AWS -Umgebung versucht, eine Domain abzufragen, die an Phishing-Angriffen beteiligt ist. Phishing-Domains werden von jemandem eingerichtet, der sich als rechtmäßige Institution ausgibt, um Personen dazu zu bringen, sensible Daten bereitzustellen, wie beispielsweise personenbezogene Informationen, Bank- und Kreditkartendaten oder Passwörter. Ihre EC2-Instance versucht möglicherweise, sensible Daten abzurufen, die auf einer Phishing-Website gespeichert sind, oder sie versucht möglicherweise, eine Phishing-Website einzurichten. Ihre EC2-Instance wurde möglicherweise kompromittiert.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

UnauthorizedAccess:EC2/MaliciousIPCaller.Custom

Eine EC2-Instance stellt Verbindungen zu einer IP-Adresse auf einer benutzerdefinierten Bedrohungsliste her.

Standard-Schweregrad: Mittel

- Datenquelle: VPC-Flow-Protokolle

Dieses Ergebnis informiert Sie darüber, dass eine EC2-Instance in Ihrer AWS Umgebung mit einer IP-Adresse kommuniziert, die in einer von Ihnen hochgeladenen Bedrohungsliste enthalten ist. In GuardDuty besteht eine Bedrohungsliste aus bekannten schädlichen IP-Adressen. GuardDuty generiert Ergebnisse basierend auf hochgeladenen Bedrohungslisten. Die Bedrohungsliste, die zum Generieren dieser Suche verwendet wird, ist in den Erkenntnisdetails aufgeführt.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

UnauthorizedAccess:EC2/MetadataDNSRebind

Eine EC2-Instance führt DNS-Abrufe durch, die in den Instance-Metadatenservice aufgelöst werden.

Standard-Schweregrad: Hoch

- Datenquelle: DNS-Protokolle

Dieses Ergebnis informiert Sie darüber, dass eine EC2-Instance in Ihrer AWS Umgebung eine Domain abfragt, die in die EC2-Metadaten-IP-Adresse (169.254.169.254) aufgelöst wird. Eine solche DNS-Abfrage kann darauf hinweisen, dass die Instance das Ziel einer DNS-Neubindung-Technik ist. Diese Technik kann verwendet werden, um Metadaten von einer EC2-Instance abzurufen, einschließlich der mit der Instance verknüpften IAM-Anmeldeinformationen.

Bei der DNS-Neubindung wird eine Anwendung, die auf der EC2-Instance läuft, dazu gebracht, Rückgabedaten von einer URL zu laden, wobei der Domainname in der URL in die IP-Adresse der EC2-Metadaten (169.254.169.254) aufgelöst wird. Dies bewirkt, dass die Anwendung auf EC2-Metadaten zugreift und sie möglicherweise für den Angreifer verfügbar macht.

Der Zugriff auf EC2-Metadaten mit DNS-Neubindung ist nur möglich, wenn auf der EC2-Instance eine anfällige Anwendung ausgeführt wird, die das Einfügen von URLs ermöglicht, oder wenn ein menschlicher Benutzer in einem Webbrowser, der auf der EC2-Instance ausgeführt wird, auf die URL zugreift.

Empfehlungen zur Abhilfe:

Prüfen Sie als Reaktion auf diese Erkenntnis, ob auf der EC2-Instance eine anfällige Anwendung ausgeführt wird, oder ob ein menschlicher Benutzer über einen Browser auf die im Ergebnis angegebene Domain zugegriffen hat. Wenn die Ursache eine anfällige Anwendung ist, beheben Sie die Schwachstelle. Wenn ein Benutzer die identifizierte Domain aufgerufen hat, blockieren Sie die Domain oder verhindern Sie, dass Benutzer darauf zugreifen. Wenn Sie in dieser Erkenntnis einen Zusammenhang mit einem der obigen Fälle feststellen, sollten Sie die der EC2-Instance zugeordnete Sitzung widerrufen.

Manche AWS Kunden ordnen die Metadaten-IP-Adresse bewusst einem Domainnamen auf ihren autoritativen DNS-Servern zu. Wenn dies in Ihrer -Umgebung der Fall ist, empfehlen wir, für diese Erkenntnis eine Unterdrückungsregel festzulegen. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Ergebnistyp mit dem Wert `UnauthorizedAccess:EC2/MetaDataDNSRebind` verwenden. Das zweite Filterkriterium sollte die DNS-Anforderungs-Domain sein, und der Wert sollte mit der Domain übereinstimmen, die Sie der Metadaten-IP-Adresse zugeordnet haben (169.254.169.254). Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln in GuardDuty.

UnauthorizedAccess:EC2/RDPBruteForce

Eine EC2-Instance war an RDP-Brute-Force-Angriffen beteiligt.

Standard-Schweregrad: Niedrig*

> **Note**
>
> Der Schweregrad dieser Erkenntnis ist niedrig, wenn Ihre EC2-Instance das Ziel eines Brute-Force-Angriffs war. Der Schweregrad dieser Erkenntnis ist hoch, wenn Ihre EC2-Instance der zum Ausführen eines Brute-Force-Angriffs verwendete Akteur ist.

- Datenquelle: VPC-Flow-Protokolle

Dieses Ergebnis informiert Sie darüber, dass eine EC2-Instance in Ihrer AWS Umgebung an einem Brute-Force-Angriff beteiligt war, der darauf abzielte, Passwörter für RDP-Dienste auf Systemen zu erhalten. Windows-based Dies kann auf einen unbefugten Zugriff auf Ihre AWS -Ressourcen hinweisen.

Empfehlungen zur Abhilfe:

Wenn die Ressourcenrolle Ihrer Instance `ACTOR` lautet, bedeutet dies, dass Ihre Instance zum Ausführen von RDP-Brute-Force-Angriffen verwendet wurde. Außer, wenn diese Instance einen legitimen Grund hat, die IP-Adresse zu kontaktieren, die als `Target` aufgeführt ist, wird empfohlen, davon auszugehen, dass Ihre Instance kompromittiert wurde, und die in Behebung einer potenziell kompromittierten Amazon EC2-Instance aufgeführten Maßnahmen zu ergreifen.

Wenn die Ressourcenrolle Ihrer Instance `TARGET` lautet, kann dieses Problem behoben werden, indem Sie Ihren RDP-Port mit Hilfe von Sicherheitsgruppen, ACLs oder Firewalls nur für vertrauenswürdige IPs sichern. Weitere Informationen finden Sie unter Tipps zur Sicherung Ihrer EC2-Instances (Linux).

UnauthorizedAccess:EC2/SSHBruteForce

Eine EC2-Instance war an SSH-Brute-Force-Angriffen beteiligt.

Standard-Schweregrad: Niedrig*

> **Note**
>
> Der Schweregrad dieser Erkenntnis ist niedrig, wenn ein Brute-Force-Angriff auf eine Ihrer EC2-Instances abzielt. Der Schweregrad dieser Erkenntnis ist hoch, wenn Ihre EC2-Instance verwendet wird, um einen Brute-Force-Angriff durchzuführen.

- Datenquelle: VPC-Flow-Protokolle

Dieses Ergebnis informiert Sie darüber, dass eine EC2-Instance in Ihrer AWS Umgebung an einem Brute-Force-Angriff beteiligt war, der darauf abzielte, Passwörter für SSH-Dienste auf Systemen zu erhalten. Linux-based Dies kann auf einen unbefugten Zugriff auf Ihre AWS -Ressourcen hinweisen.

> **Note**
>
> Dieses Ergebnis wird nur über den -Überwachungsdatenverkehr auf Port 22 generiert. Wenn Ihre SSH-Services so konfiguriert sind, dass sie andere Ports verwenden, wird diese Erkenntnis nicht generiert.

Empfehlungen zur Abhilfe:

Wenn das Ziel des Brute-Force-Versuchs ein Bastion-Host ist, kann dies ein erwartetes Verhalten für Ihre Umgebung sein. AWS In diesem Fall sollten Sie für diese Erkenntnis eine Unterdrückungsregel einrichten. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Ergebnistyp mit dem Wert `UnauthorizedAccess:EC2/SSHBruteForce` verwenden. Das zweite Filterkriterium sollte der oder den Instances entsprechen, die als Bastion-Host eingesetzt werden. Sie können entweder das Attribut Instance-Image-ID oder das Attribut Tag verwenden, abhängig davon, welches Kriterium mit den Instances identifiziert werden kann, die diese Tools hosten. Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln in GuardDuty.

Wenn diese Aktivitäten für Ihre Umgebung nicht erwartet werden und die Ressourcenrolle Ihrer Instance `TARGET` lautet, kann diese Erkenntnis behoben werden, indem Sie Ihren SSH-Port mit Hilfe von Sicherheitsgruppen, ACLs oder Firewalls nur für vertrauenswürdige IPs sichern. Weitere Informationen finden Sie unter Tipps zur Sicherung Ihrer EC2-Instances (Linux).

Wenn die Ressourcenrolle Ihrer Instance `ACTOR` lautet, bedeutet dies, dass die Instance zum Ausführen von SSH-Brute-Force-Angriffen verwendet wurde. Außer, wenn diese Instance einen legitimen Grund hat, die IP-Adresse zu kontaktieren, die als `Target` aufgeführt ist, wird empfohlen, davon auszugehen, dass Ihre Instance kompromittiert wurde, und die in Behebung einer potenziell kompromittierten Amazon EC2-Instance aufgeführten Maßnahmen zu ergreifen.

UnauthorizedAccess:EC2/TorClient

Ihre EC2-Instance stellt Verbindungen mit einem Tor Guard oder einem Authority-Knoten her.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Dieses Ergebnis informiert Sie darüber, dass eine EC2-Instance in Ihrer AWS Umgebung Verbindungen zu einem Tor Guard- oder einem Authority-Knoten herstellt. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Tor Guards und Authority-Knoten fungieren als erste Gateways in ein Tor-Netzwerk. Dieser Datenverkehr kann darauf hinweisen, dass diese EC2-Instance als Client in einem Tor-Netzwerk fungiert. Dieses Ergebnis kann auf einen unbefugten Zugriff auf Ihre AWS Ressourcen hinweisen, mit der Absicht, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

UnauthorizedAccess:EC2/TorRelay

Ihre EC2-Instance stellt Verbindungen mit einem Tor-Netzwerk als Tor-Relais her.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Dieses Ergebnis informiert Sie darüber, dass eine EC2-Instance in Ihrer AWS Umgebung Verbindungen zu einem Tor-Netzwerk auf eine Weise herstellt, die darauf hindeutet, dass sie als Tor-Relay fungiert. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Tor-Relays erhöhen die Anonymität der Kommunikation, indem sie den möglicherweise illegalen Datenverkehr des Kunden von einem Tor-Relay zu einem anderen weiterleiten.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

GuardDuty IAM findet Typen

Die folgenden Erkenntnisse beziehen sich auf IAM-Entitäten und Zugriffsschlüssel und weisen immer den Ressourcentyp `AccessKey` auf. Der Schweregrad und die Details der Erkenntnisse unterscheiden sich je nach Erkenntnistyp.

Die hier aufgeführten Erkenntnisse beinhalten die Datenquellen und Modelle, die zur Generierung dieses Erkenntnistyps verwendet wurden. Weitere Informationen finden Sie unter GuardDuty grundlegende Datenquellen.

Für alle IAM-related Ergebnisse empfehlen wir Ihnen, die betreffende Entität zu untersuchen und sicherzustellen, dass ihre Berechtigungen der bewährten Methode der geringsten Zugriffsrechte entsprechen. Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen zur Behebung von Erkenntnissen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

Themen

- CredentialAccess:IAMUser/AnomalousBehavior
- CredentialAccess:IAMUser/CompromisedCredentials
- DefenseEvasion:IAMUser/AnomalousBehavior
- DefenseEvasion:IAMUser/BedrockLoggingDisabled
- Discovery:IAMUser/AnomalousBehavior
- Exfiltration:IAMUser/AnomalousBehavior
- Impact:IAMUser/AnomalousBehavior
- InitialAccess:IAMUser/AnomalousBehavior
- PenTest:IAMUser/KaliLinux
- PenTest:IAMUser/ParrotLinux
- PenTest:IAMUser/PentooLinux
- Persistence:IAMUser/AnomalousBehavior
- Policy:IAMUser/RootCredentialUsage
- Policy:IAMUser/ShortTermRootCredentialUsage
- PrivilegeEscalation:IAMUser/AnomalousBehavior
- Recon:IAMUser/MaliciousIPCaller

- Recon:IAMUser/MaliciousIPCaller.Custom
- Recon:IAMUser/TorIPCaller
- Stealth:IAMUser/CloudTrailLoggingDisabled
- Stealth:IAMUser/PasswordPolicyChange
- UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
- UnauthorizedAccess:IAMUser/MaliciousIPCaller
- UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom
- UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS
- UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS
- UnauthorizedAccess:IAMUser/TorIPCaller

CredentialAccess:IAMUser/AnomalousBehavior

Eine API, die verwendet wird, um Zugriff auf eine zu erhalten AWS Die Umgebung wurde auf anomale Weise aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: Management-Ereignis CloudTrail

Diese Erkenntnis informiert Sie darüber, dass in Ihrem Konto eine ungewöhnliche API-Anfrage beobachtet wurde. Diese Erkenntnis kann eine einzelne API oder eine Reihe verwandter API-Anfragen beinhalten, die in unmittelbarer Nähe von einer einzelnen Benutzeridentität gestellt wurden. Die beobachtete API wird häufig mit der Phase des Zugriffs auf Anmeldeinformationen in Verbindung gebracht, wenn ein Angreifer versucht, Passwörter, Benutzernamen und Zugriffsschlüssel für Ihre Umgebung zu sammeln. Die APIs in dieser Kategorie sind `GetPasswordDataGetSecretValue`,`BatchGetSecretValue`, und`GenerateDbAuthToken`.

Diese API-Anfrage wurde vom Modell für maschinelles Lernen (ML) zur Erkennung GuardDuty von Anomalien als anomal identifiziert. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Taktiken von Angreifern in Verbindung gebracht werden.

Das ML-Modell verfolgt verschiedene Faktoren der API-Anfrage, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und die spezifische API, die angefordert wurde. Einzelheiten darüber, welche Faktoren der API-Anfrage für die Benutzeridentität, die die Anfrage aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

CredentialAccess:IAMUser/CompromisedCredentials

Ein IAM-Zugriffsschlüssel wurde von Amazon Threat Intelligence als potenziell kompromittiert identifiziert.

Standard-Schweregrad: Hoch

- Funktion: Im grundlegenden Datenquellenschutz enthalten

Vollständige Beschreibung:

Dieses Ergebnis informiert Sie darüber, dass ein Ihrem AWS Konto zugeordneter IAM-Zugriffsschlüssel von Amazon Threat Intelligence als potenziell gefährdet eingestuft wurde. Die kompromittierten Anmeldeinformationen wurden dann verwendet, um API-Operationen in Ihrer Umgebung aufzurufen. AWS Die Liste der API-Aufrufe, die mit den kompromittierten Anmeldeinformationen getätigt wurden, ist zusammen mit der Anzahl und den Zeitstempeln jedes Aufrufs, dem involvierten Zugriffsschlüssel und der Quell-IP-Adresse in den Erkenntnisdetails enthalten.

Die Sicherheitslücken bei diesem Befund wurden von Amazon Threat Intelligence identifiziert. AWS überwacht potenziell kompromittierte Anmeldedaten anhand von Nutzungsmustern und generiert dieses Ergebnis, wenn beobachtet wird, dass solche Zugangsdaten verwendet werden.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

DefenseEvasion:IAMUser/AnomalousBehavior

Eine API, die zur Umgehung von Abwehrmaßnahmen verwendet wird, wurde auf anomale Weise aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: Verwaltungsereignis CloudTrail

Diese Erkenntnis informiert Sie darüber, dass in Ihrem Konto eine ungewöhnliche API-Anfrage beobachtet wurde. Diese Erkenntnis kann eine einzelne API oder eine Reihe verwandter API-Anfragen umfassen, die in der Nähe von einer einzelnen Benutzeridentität getätigt wurden. Die beobachtete API wird häufig mit Umgehungstaktiken in Verbindung gebracht, bei denen ein Gegner versucht, seine Spuren zu verwischen und nicht entdeckt zu werden. Bei APIs in dieser Kategorie handelt es sich in der Regel um Lösch-, Deaktivierungs- oder Stoppvorgänge wie `DeleteFlowLogs`, `DisableAlarmActions` oder `StopLogging`.

Diese API-Anfrage wurde vom Modell GuardDuty des maschinellen Lernens (ML) zur Erkennung von Anomalien als anomal identifiziert. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Taktiken von Angreifern in Verbindung gebracht werden. Das ML-Modell verfolgt verschiedene Faktoren der API-Anfrage, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und die spezifische API, die angefordert wurde. Einzelheiten darüber, welche Faktoren der API-Anfrage für die Benutzeridentität, die die Anfrage aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

DefenseEvasion:IAMUser/BedrockLoggingDisabled

Die Protokollierung für Amazon Bedrock wurde deaktiviert.

Standard-Schweregrad: Mittel

- Datenquelle: Verwaltungsereignisse CloudTrail

Diese Erkenntnis informiert Sie darüber, dass die Protokollierung für Bedrock-Modellaufrufe in Ihrem Konto deaktiviert wurde. Dabei kann es sich um den Versuch eines Angreifers handeln, böswillige Aktivitäten wie Datenexfiltration oder Missbrauch von KI-Modellen zu verbergen. Durch die Deaktivierung der Protokollierung wird der Einblick in die an Modelle gesendeten Daten und deren Verwendung entfernt.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

Discovery:IAMUser/AnomalousBehavior

Eine API, die häufig zum Auffinden von Ressourcen verwendet wird, wurde auf ungewöhnliche Weise aufgerufen.

Standard-Schweregrad: Niedrig

- Datenquelle: CloudTrail Verwaltungsereignis

Diese Erkenntnis informiert Sie darüber, dass in Ihrem Konto eine ungewöhnliche API-Anfrage beobachtet wurde. Diese Erkenntnis kann eine einzelne API oder eine Reihe verwandter API-Anfragen umfassen, die in der Nähe von einer einzelnen Benutzeridentität getätigt wurden. Die beobachtete API wird häufig mit der Erkennungsphase eines Angriffs in Verbindung gebracht, in der ein Gegner Informationen sammelt, um festzustellen, ob Ihre AWS Umgebung für einen umfassenderen Angriff anfällig ist. APIs in dieser Kategorie sind in der Regel Get-, Describe- oder List-Vorgänge wie `DescribeInstances`, `GetRolePolicy` oder `ListAccessKeys`.

Diese API-Anfrage wurde vom Modell des maschinellen Lernens (ML) zur Erkennung GuardDuty von Anomalien als anomal identifiziert. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Taktiken von Angreifern in Verbindung gebracht werden. Das ML-Modell verfolgt verschiedene Faktoren der API-Anfrage, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und die spezifische API, die angefordert wurde. Einzelheiten darüber, welche Faktoren der API-Anfrage für die Benutzeridentität, die die Anfrage aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

Exfiltration:IAMUser/AnomalousBehavior

Eine API, die häufig verwendet wird, um Daten von einem zu sammeln AWS Die Umgebung wurde auf anomale Weise aufgerufen.

Standard-Schweregrad: Hoch

- Datenquelle: Management-Ereignis CloudTrail

Diese Erkenntnis informiert Sie darüber, dass in Ihrem Konto eine ungewöhnliche API-Anfrage beobachtet wurde. Diese Erkenntnis kann eine einzelne API oder eine Reihe verwandter API-Anfragen umfassen, die in der Nähe von einer einzelnen Benutzeridentität getätigt wurden. Die beobachtete API wird üblicherweise mit Exfiltrationstaktiken in Verbindung gebracht, bei denen ein Angreifer versucht, Daten aus Ihrem Netzwerk zu sammeln, indem er sie verpackt und verschlüsselt, um eine Entdeckung zu vermeiden. APIs für diesen Erkenntnistyp sind Verwaltungsvorgänge (Steuerebene) und beziehen sich in der Regel auf S3, Snapshots und Datenbanken wie `PutBucketReplication`, `CreateSnapshot` oder `RestoreDBInstanceFromDBSnapshot`.

Diese API-Anfrage wurde vom Modell GuardDuty des maschinellen Lernens (ML) zur Erkennung von Anomalien als anomal identifiziert. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Taktiken von Angreifern in Verbindung gebracht werden. Das ML-Modell verfolgt verschiedene Faktoren der API-Anfrage, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und die spezifische API, die angefordert wurde. Einzelheiten darüber, welche Faktoren der API-Anfrage für die Benutzeridentität, die die Anfrage aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

Impact:IAMUser/AnomalousBehavior

Eine API, die häufig verwendet wird, um Daten oder Prozesse in einem zu manipulieren AWS Die Umgebung wurde auf anomale Weise aufgerufen.

Standard-Schweregrad: Hoch

- Datenquelle: Management-Ereignis CloudTrail

Diese Erkenntnis informiert Sie darüber, dass in Ihrem Konto eine ungewöhnliche API-Anfrage beobachtet wurde. Diese Erkenntnis kann eine einzelne API oder eine Reihe verwandter API-Anfragen umfassen, die in der Nähe von einer einzelnen Benutzeridentität getätigt wurden. Die beobachtete API wird in der Regel mit Angriffstaktiken in Verbindung gebracht, bei denen ein Angreifer versucht, den Betrieb zu stören und Daten in Ihrem Konto zu manipulieren, zu unterbrechen oder zu zerstören. APIs für diese Art der Suche sind in der Regel Lösch-, Aktualisierungs- oder Stellvorgänge wie `DeleteSecurityGroup`, `UpdateUser` oder `PutBucketPolicy`.

Diese API-Anfrage wurde vom Modell GuardDuty des maschinellen Lernens (ML) zur Erkennung von Anomalien als anomal identifiziert. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Taktiken von Angreifern in Verbindung gebracht werden. Das ML-Modell verfolgt verschiedene Faktoren der API-Anfrage, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und die spezifische API, die angefordert wurde. Einzelheiten darüber, welche Faktoren der API-Anfrage für die Benutzeridentität, die die Anfrage aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

InitialAccess:IAMUser/AnomalousBehavior

Eine API, die häufig verwendet wird, um unbefugten Zugriff auf eine AWS Die Umgebung wurde auf anomale Weise aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: Management-Ereignis CloudTrail

Diese Erkenntnis informiert Sie darüber, dass in Ihrem Konto eine ungewöhnliche API-Anfrage beobachtet wurde. Diese Erkenntnis kann eine einzelne API oder eine Reihe verwandter API-Anfragen umfassen, die in der Nähe von einer einzelnen Benutzeridentität getätigt wurden. Die beobachtete API wird häufig mit der ersten Zugriffsphase eines Angriffs in Verbindung gebracht, wenn ein Angreifer versucht, Zugriff auf Ihre Umgebung zu erhalten. Bei APIs in dieser Kategorie handelt es sich in der Regel um Get Token- oder Sitzungsoperationen wie`StartSession`, oder`GetAuthorizationToken`.

Diese API-Anfrage wurde vom Modell GuardDuty des maschinellen Lernens (ML) zur Erkennung von Anomalien als anomal identifiziert. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Taktiken von Angreifern in Verbindung gebracht werden. Das ML-Modell verfolgt verschiedene Faktoren der API-Anfrage, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und die spezifische API, die angefordert wurde. Einzelheiten darüber, welche Faktoren der API-Anfrage für die Benutzeridentität, die die Anfrage aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

PenTest:IAMUser/KaliLinux

Eine API wurde von einem Kali Linux-Computer aus aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: Management-Ereignis CloudTrail

Dieses Ergebnis informiert Sie darüber, dass ein Computer, auf dem Kali Linux ausgeführt wird, API-Aufrufe mit Anmeldeinformationen durchführt, die zu dem aufgelisteten AWS Konto in Ihrer Umgebung gehören. Kali Linux ist ein beliebtes Tool für Penetrationstests, das von Sicherheitsexperten verwendet wird, um Schwachstellen in EC2-Instances zu erkennen, für die Patches erforderlich sind. Angreifer verwenden dieses Tool auch, um Sicherheitslücken in der EC2-Konfiguration zu finden und sich unbefugten Zugriff auf Ihre AWS Umgebung zu verschaffen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

PenTest:IAMUser/ParrotLinux

Eine API wurde von einem Parrot-Security-Linux-Computer aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Management-Ereignis

Dieses Ergebnis informiert Sie darüber, dass ein Computer, auf dem Parrot Security Linux ausgeführt wird, API-Aufrufe mit Anmeldeinformationen durchführt, die zu dem in Ihrer Umgebung aufgeführten AWS Konto gehören. Parrot Security Linux ist ein beliebtes Tool für Penetrationstests, das von Sicherheitsexperten verwendet wird, um Schwachstellen in EC2-Instances zu erkennen, für die Patches erforderlich sind. Angreifer nutzen dieses Tool auch, um Schwachstellen in der EC2-Konfiguration ausfindig zu machen und sich unbefugten Zugriff auf Ihre AWS Umgebung zu verschaffen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

PenTest:IAMUser/PentooLinux

Eine API wurde von einem Pentoo-Linux-Computer aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Management-Ereignis

Dieses Ergebnis informiert Sie darüber, dass ein Computer, auf dem Pentoo Linux ausgeführt wird, API-Aufrufe mit Anmeldeinformationen durchführt, die zu dem aufgelisteten AWS Konto in Ihrer Umgebung gehören. Pentoo Linux ist ein beliebtes Tool für Penetrationstests, das von Sicherheitsexperten verwendet wird, um Schwachstellen in EC2-Instances zu erkennen, für die

Patches erforderlich sind. Angreifer verwenden dieses Tool auch, um Sicherheitslücken in der EC2-Konfiguration zu finden und sich unbefugten Zugriff auf Ihre AWS Umgebung zu verschaffen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

Persistence:IAMUser/AnomalousBehavior

Eine API, die häufig verwendet wird, um den unbefugten Zugriff auf eine AWS Die Umgebung wurde auf anomale Weise aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: Management-Ereignis CloudTrail

Diese Erkenntnis informiert Sie darüber, dass in Ihrem Konto eine ungewöhnliche API-Anfrage beobachtet wurde. Diese Erkenntnis kann eine einzelne API oder eine Reihe verwandter API-Anfragen umfassen, die in der Nähe von einer einzelnen Benutzeridentität getätigt wurden. Die beobachtete API wird häufig mit Persistenztaktiken in Verbindung gebracht, bei denen sich ein Angreifer Zugriff auf Ihre Umgebung verschafft hat und versucht, diesen Zugriff aufrechtzuerhalten. APIs in dieser Kategorie sind in der Regel Erstellungs-, Import- oder Änderungsvorgänge wie `CreateAccessKey`, `ImportKeyPair` oder `ModifyInstanceAttribute`.

Diese API-Anfrage wurde vom Modell GuardDuty des maschinellen Lernens (ML) zur Erkennung von Anomalien als anomal identifiziert. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Taktiken von Angreifern in Verbindung gebracht werden. Das ML-Modell verfolgt verschiedene Faktoren der API-Anfrage, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und die spezifische API, die angefordert wurde. Einzelheiten darüber, welche Faktoren der API-Anfrage für die Benutzeridentität, die die Anfrage aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

Policy:IAMUser/RootCredentialUsage

Eine API wurde über Root-Benutzer-Anmeldeinformationen aufgerufen.

Standard-Schweregrad: Niedrig

- Datenquelle: CloudTrail Verwaltungsereignisse oder CloudTrail Datenereignisse für S3

Diese Erkenntnis informiert Sie darüber, dass die Root-Benutzer-Anmeldeinformationen des in Ihrer Umgebung angeführten AWS-Konto -Kontos verwendet werden, um Anforderungen an AWS -Services zu erstellen. Es wird empfohlen, dass Benutzer niemals die Anmeldedaten eines Root-Benutzers verwenden, um auf AWS Dienste zuzugreifen. Stattdessen sollten für den Zugriff auf AWS Dienste die temporären Anmeldeinformationen mit den geringsten Rechten von AWS -Security-Token-Service (STS) verwendet werden. Für Situationen, in denen AWS STS nicht unterstützt wird, werden IAM-Benutzeranmeldeinformationen empfohlen. Weitere Informationen finden Sie unter Bewährte Methoden für IAM.

> **Note**
>
> Wenn der S3-Schutz für das Konto aktiviert ist, kann dieses Ergebnis als Reaktion auf die Versuche generiert werden, S3-Datenebenenoperationen auf Amazon S3-Ressourcen mithilfe der Root-Benutzer-Anmeldeinformationen von auszuführen. AWS-Konto Der verwendete API-Aufruf wird in den Erkenntnisdetails aufgeführt. Wenn S3 Protection nicht aktiviert ist, kann diese Feststellung nur durch Ereignisprotokoll-APIs ausgelöst werden. Weitere Informationen zu S3 Protection finden Sie unterS3-Schutz.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

Policy:IAMUser/ShortTermRootCredentialUsage

Eine API wurde mithilfe eingeschränkter Root-Benutzer-Anmeldeinformationen aufgerufen.

Standard-Schweregrad: Niedrig

- Datenquelle: AWS CloudTrail Verwaltungsereignisse oder AWS CloudTrail Datenereignisse für S3

Dieses Ergebnis informiert Sie darüber, dass eingeschränkte Benutzeranmeldeinformationen, die für die AWS-Konto in Ihrer Umgebung aufgeführten Benutzer erstellt wurden, verwendet werden, um Anfragen an zu stellen AWS-Services. Es wird empfohlen, Root-Benutzeranmeldeinformationen nur für Aufgaben zu verwenden, für die Root-Benutzeranmeldeinformationen erforderlich sind.

Wenn möglich, greifen Sie auf die zu, AWS-Services indem Sie IAM-Rollen mit den geringsten Rechten und temporären Anmeldeinformationen von AWS -Security-Token-Service (AWS STS) verwenden. In Szenarien, in denen AWS STS dies nicht unterstützt wird, empfiehlt es sich, IAM-Benutzeranmeldeinformationen zu verwenden. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden in IAM und Bewährte Methoden für Root-Benutzer für Sie AWS-Konto im IAM-Benutzerhandbuch.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

PrivilegeEscalation:IAMUser/AnomalousBehavior

Eine API, die häufig verwendet wird, um hochrangige Berechtigungen für einen zu erhalten AWS Die Umgebung wurde auf ungewöhnliche Weise aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: Verwaltungsereignisse CloudTrail

Diese Erkenntnis informiert Sie darüber, dass in Ihrem Konto eine ungewöhnliche API-Anfrage beobachtet wurde. Diese Erkenntnis kann eine einzelne API oder eine Reihe verwandter API-Anfragen umfassen, die in der Nähe von einer einzelnen Benutzeridentität getätigt wurden. Die beobachtete API wird häufig mit Taktiken zur Eskalation von Rechten in Verbindung gebracht, bei denen ein Angreifer versucht, Berechtigungen auf höherer Ebene für eine Umgebung zu erlangen. APIs in dieser Kategorie beinhalten in der Regel Vorgänge, die IAM-Richtlinien, Rollen und Benutzer ändern, wie `AssociateIamInstanceProfile`, `AddUserToGroup` oder `PutUserPolicy`.

Diese API-Anfrage wurde vom Modell GuardDuty des maschinellen Lernens (ML) zur Erkennung von Anomalien als anomal identifiziert. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus

und identifiziert anomale Ereignisse, die mit Taktiken von Angreifern in Verbindung gebracht werden. Das ML-Modell verfolgt verschiedene Faktoren der API-Anfrage, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und die spezifische API, die angefordert wurde. Einzelheiten darüber, welche Faktoren der API-Anfrage für die Benutzeridentität, die die Anfrage aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

Recon:IAMUser/MaliciousIPCaller

Eine API wurde von einer bekannten böswilligen IP-Adresse aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: Verwaltungsereignisse CloudTrail

Diese Erkenntnis informiert Sie, dass ein API-Vorgang, der AWS -Ressourcen auflisten oder beschreiben kann, von einer IP-Adresse aufgerufen wurde, die in einer Bedrohungsliste enthalten ist. Ein Angreifer kann gestohlene Anmeldedaten verwenden, um diese Art der Erkundung Ihrer AWS Ressourcen durchzuführen, um wertvollere Anmeldeinformationen zu finden oder die Fähigkeiten der bereits vorhandenen Anmeldeinformationen zu ermitteln.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

Recon:IAMUser/MaliciousIPCaller.Custom

Eine API wurde von einer bekannten böswilligen IP-Adresse aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: Verwaltungsereignisse CloudTrail

Diese Erkenntnis informiert Sie, dass ein API-Vorgang, der AWS -Ressourcen auflisten oder beschreiben kann, von einer IP-Adresse aufgerufen wurde, die in einer benutzerdefinierten Bedrohungsliste enthalten ist. Die verwendete Bedrohungsliste wird in den Erkenntnisdetails aufgeführt. Ein Angreifer könnte gestohlene Anmeldeinformationen verwenden, um diese Art der Erkundung Ihrer AWS Ressourcen durchzuführen, um wertvollere Anmeldeinformationen zu finden oder die Fähigkeiten der bereits vorhandenen Anmeldeinformationen zu ermitteln.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

Recon:IAMUser/TorIPCaller

Eine API wurde von einer IP-Adresse eines Tor-Ausgangsknotens aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: Verwaltungsereignisse CloudTrail

Diese Erkenntnis informiert Sie, dass ein API-Vorgang, der Ihre AWS -Ressourcen auflisten oder beschreiben kann, von einer IP-Adresse eines Tor-Ausgangsknotens aufgerufen wurde. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese nach dem Zufallsprinzip durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Ein Angreifer würde Tor verwenden, um seine wahre Identität zu verschleiern.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

Stealth:IAMUser/CloudTrailLoggingDisabled

AWS CloudTrail Die Protokollierung wurde deaktiviert.

Standard-Schweregrad: Niedrig

- Datenquelle: CloudTrail Verwaltungsereignisse

Dieses Ergebnis informiert Sie darüber, dass ein CloudTrail Pfad in Ihrer AWS Umgebung deaktiviert wurde. Dabei kann es sich um den Versuch eines Angreifers handeln, die Protokollierung seiner Aktivitäten zu deaktivieren, indem er alle Spuren beseitigt, während er mit böswilliger Absicht Zugriff auf die AWS -Ressourcen erlangt. Diese Erkenntnis kann durch das erfolgreiche Löschen oder Aktualisieren eines Trails ausgelöst werden. Dieses Ergebnis kann auch durch das erfolgreiche Löschen eines S3-Buckets ausgelöst werden, in dem die Protokolle eines zugehörigen Trails gespeichert sind GuardDuty.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

Stealth:IAMUser/PasswordPolicyChange

Die Passwortrichtlinie des Kontos wurde geschwächt.

Standard-Schweregrad: Niedrig*

> **Note**
>
> Der Schweregrad dieser Erkenntnis kann je nach Schweregrad der an der Passwortrichtlinie vorgenommenen Änderungen Niedrig, Mittel oder Hoch sein.

- Datenquelle: CloudTrail Verwaltungsereignisse

Die AWS Kontopasswortrichtlinie wurde für das aufgelistete Konto in Ihrer AWS Umgebung geschwächt. Beispiel: Sie wurde gelöscht oder aktualisiert und erfordert jetzt weniger Zeichen, keine Sonderzeichen und Zahlen mehr oder das Ablaufdatum des Passworts musste verlängert werden. Diese Feststellung kann auch durch einen Versuch ausgelöst werden, Ihre AWS Kontopasswortrichtlinie zu aktualisieren oder zu löschen. Die AWS Kontopasswortrichtlinie definiert die Regeln, die regeln, welche Arten von Passwörtern für Ihre IAM-Benutzer festgelegt werden können. Eine schwächere Passwortrichtlinie ermöglicht das Erstellen von Passwörtern, die leicht zu merken und möglicherweise einfacher zu erraten sind. Dadurch entsteht ein Sicherheitsrisiko.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B

Mehrere weltweit erfolgreiche Konsolenanmeldungen wurden beobachtet.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Verwaltungsereignisse

Diese Erkenntnis informiert Sie darüber, dass mehrere erfolgreiche Konsolenanmeldungen für denselben IAM-Benutzer zur etwa gleichen Zeit an verschiedenen geografischen Standorten beobachtet wurden. Solche anomalen und riskanten Zugriffsmuster weisen auf einen potenziellen unbefugten Zugriff auf Ihre AWS Ressourcen hin.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS

Anmeldeinformationen, die exklusiv für eine EC2-Instance mithilfe einer Instance-Startrolle erstellt wurden, werden von einem anderen Konto innerhalb von AWS.

Standard-Schweregrad: Hoch*

> **Note**
>
> Der Standard-Schweregrad diese Erkenntnis ist Hoch. Wenn die API jedoch von einem Konto aufgerufen wurde, das zu Ihrer AWS Umgebung gehört, ist der Schweregrad Mittel.

- Datenquelle: CloudTrail Verwaltungsereignisse oder CloudTrail Datenereignisse für S3

Mit dieser Erkenntnis werden Sie informiert, wenn Ihre Anmeldeinformationen für die Amazon-EC2-Instance zum Aufrufen von APIs von einer IP-Adresse oder einem Amazon-VPC-Endpunkt verwendet werden, die einem anderen AWS -Konto gehört als dem, in dem die zugehörige Amazon-EC2-Instance ausgeführt wird. Die VPC-Endpunkterkennung ist nur für Services verfügbar, die Netzwerkaktivitätsereignisse für VPC-Endpunkte unterstützen. Informationen zu Services, die Netzwerkaktivitätsereignisse für VPC-Endpunkte unterstützen, finden Sie im Benutzerhandbuch für AWS CloudTrail unter Protokollieren von Netzwerkaktivitätsereignissen.

AWS empfiehlt nicht, temporäre Anmeldeinformationen außerhalb der Entität weiterzuverteilen, die sie erstellt hat (z. B. AWS Anwendungen, Amazon EC2 oder). AWS Lambda Allerdings können autorisierte Benutzer Anmeldeinformationen aus ihren Amazon-EC2-Instances exportieren, um legitime API-Aufrufe durchzuführen. Wenn das `remoteAccountDetails.Affiliated` Feld lautet, wurde `True` die API von einem Konto aufgerufen, das demselben Administratorkonto zugeordnet ist. Um einen möglichen Angriff auszuschließen und die Legitimität der Aktivität zu überprüfen, wenden Sie sich an den AWS-Konto Eigentümer oder IAM-Principal, dem diese Anmeldeinformationen zugewiesen sind.

> **Note**
>
> Wenn von einem Remote-Konto aus fortgesetzte Aktivitäten GuardDuty beobachtet werden, erkennt das Machine-Learning-Modell (ML) dies als erwartetes Verhalten. Daher GuardDuty wird dieses Ergebnis nicht mehr für Aktivitäten von diesem Remote-Konto aus generiert. GuardDuty wird weiterhin Erkenntnisse über neues Verhalten von anderen Remote-Konten generieren und erlernte Remote-Accounts neu bewerten, wenn sich das Verhalten im Laufe der Zeit ändert.

Empfehlungen zur Abhilfe:

Dieses Ergebnis wird generiert, wenn AWS API-Anfragen innerhalb AWS einer Amazon EC2-Instance außerhalb von Ihnen gestellt werden AWS-Konto, wobei die Sitzungsanmeldedaten Ihrer Amazon EC2-Instance verwendet werden. Es kann üblich sein, beispielsweise bei der Transit Gateway-Architektur in einer https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/transit-vpc-solution.html Hub-and-Spoke-Konfiguration, den Datenverkehr über eine einzelne Hub-VPC mit Service-Endpunkten weiterzuleiten. AWS Wenn dieses Verhalten erwartet wird, GuardDuty empfiehlt dann, eine Regel mit zwei Filterkriterien zu verwenden Unterdrückungsregeln und zu erstellen. Das erste Kriterium ist der Erkenntnistyp, in

diesem Fall UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS. Das zweite Filterkriterium ist die Remote-Konto-ID der Remote-Kontodetails.

Als Reaktion auf diese Erkenntnis können Sie den folgenden Workflow verwenden, um das weitere Vorgehen festzulegen:

1. Identifizieren Sie das betroffene Remote-Konto im Feld `service.action.awsApiCallAction.remoteAccountDetails.accountId`.
2. Stellen Sie vor `service.action.awsApiCallAction.remoteAccountDetails.affiliated` Ort fest, ob das Konto mit Ihrer GuardDuty Umgebung verknüpft ist.
3. Wenn das Konto verbunden ist, wenden Sie sich an den Eigentümer des Remote-Kontos und den Eigentümer der Anmeldeinformationen für die Amazon-EC2-Instance, um dies zu untersuchen.

   Wenn das Konto nicht verknüpft ist, müssen Sie zunächst prüfen, ob dieses Konto mit Ihrer Organisation verknüpft ist, aber nicht Teil Ihrer Umgebung mit GuardDuty mehreren Konten ist oder ob GuardDuty es in diesem Konto noch nicht aktiviert wurde. Wenden Sie sich andernfalls an den Eigentümer der Anmeldeinformationen für die Amazon-EC2-Instance, um festzustellen, ob es einen Anwendungsfall für ein Remote-Konto zur Verwendung dieser Anmeldeinformationen gibt.
4. Wenn der Eigentümer der Anmeldeinformationen das entfernte Konto nicht erkennt, wurden die Anmeldeinformationen möglicherweise von einem Bedrohungsakteur innerhalb von AWS kompromittiert. Sie sollten die unter empfohlenen Schritte ergreifenBehebung einer potenziell kompromittierten Amazon EC2-Instance, um Ihre Umgebung zu schützen.

   Darüber hinaus können Sie eine Missbrauchsmeldung an das AWS Trust and Safety-Team senden, um eine Untersuchung des Remote-Kontos einzuleiten. Wenn Sie Ihren Bericht an AWS Trust and Safety senden, geben Sie die vollständigen JSON-Details des Befundes an.

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS

Anmeldeinformationen, die über eine Instance-Startrolle ausschließlich für eine EC2-Instance erstellt wurden, werden von einer externen IP-Adresse verwendet.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Verwaltungsereignisse oder CloudTrail Datenereignisse für S3

Dieses Ergebnis informiert Sie darüber, dass ein Host außerhalb von versucht AWS hat, AWS API-Operationen mit temporären AWS Anmeldeinformationen auszuführen, die auf einer EC2-Instance in Ihrer AWS Umgebung erstellt wurden. Die aufgeführte EC2-Instance ist möglicherweise kompromittiert, und die temporären Anmeldeinformationen dieser Instance wurden möglicherweise auf einen Remote-Host außerhalb von exfiltriert. AWS AWS empfiehlt nicht, temporäre Anmeldeinformationen außerhalb der Entität weiterzuverteilen, die sie erstellt hat (z. B. AWS Anwendungen, EC2 oder Lambda). Allerdings können autorisierte Benutzer Anmeldeinformationen aus ihren EC2-Instances exportieren, um legitime API-Aufrufe durchzuführen. Um einen potenziellen Angriff auszuschließen und die Legitimität der Aktivität zu überprüfen, überprüfen Sie, ob die Verwendung von Instance-Anmeldeinformationen von der Remote-IP in der Erkenntnis erwartet wird.

> **Note**
>
> Wenn von einem Remote-Host aus fortgesetzte Aktivitäten GuardDuty beobachtet werden, erkennt das Machine-Learning-Modell (ML) dies als erwartetes Verhalten. Daher GuardDuty wird dieses Ergebnis nicht mehr für Aktivitäten von diesem Remote-Host generiert. GuardDuty generiert weiterhin Erkenntnisse über neues Verhalten von anderen Remote-Hosts und bewertet die gelernten Remote-Hosts erneut, wenn sich das Verhalten im Laufe der Zeit ändert.

Empfehlungen zur Abhilfe:

Diese Erkenntnis wird generiert, wenn das Netzwerk so konfiguriert ist, dass der Internetverkehr von einem On-Premises-Gateway und nicht von einem VPC Internet Gateway (IGW) ausgeht. Geläufige Konfigurationen, z. B. die Verwendung von AWS Outposts, oder VPC-VPN-Verbindungen, können dazu führen, dass Datenverkehr auf diese Weise weitergeleitet wird. Wenn dies ein erwartetes Verhalten ist, empfiehlt es sich, Unterdrückungsregeln zu verwenden und eine Regel zu erstellen, die aus zwei Filterkriterien besteht. Das erste Kriterium ist der Erkenntnistyp, der `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS` sein sollte. Das zweite Filterkriterium ist die IPv4-Adresse des API-Aufrufers mit der IP-Adresse oder dem CIDR-Bereich Ihres On-Premises-Internet-Gateways. Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln in GuardDuty.

> **Note**
>
> Wenn kontinuierliche Aktivitäten aus einer externen Quelle GuardDuty beobachtet werden, erkennt das maschinelle Lernmodell dieses Verhalten als erwartetes Verhalten und hört auf,

diese Ergebnisse für Aktivitäten aus dieser Quelle zu generieren. GuardDuty wird weiterhin Erkenntnisse über neues Verhalten aus anderen Quellen generieren und erlernte Quellen neu bewerten, wenn sich das Verhalten im Laufe der Zeit ändert.

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

UnauthorizedAccess:IAMUser/MaliciousIPCaller

Eine API wurde von einer bekannten böswilligen IP-Adresse aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: Ereignisse des CloudTrail Managements

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang (z. B. ein Versuch zum Starten einer EC2-Instance, Erstellen eines neuen IAM-Benutzers, Ändern Ihrer AWS -Berechtigungen usw.) von einer bekannten böswilligen IP-Adresse aufgerufen wurde. Dies kann auf unbefugten Zugriff auf AWS Ressourcen in Ihrer Umgebung hinweisen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom

Eine API wurde von einer IP-Adresse aufgerufen, die sich auf einer benutzerdefinierten Bedrohungsliste befindet.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Verwaltungsereignisse

Dieses Ergebnis informiert Sie darüber, dass ein API-Vorgang (z. B. ein Versuch, eine EC2-Instance zu starten, einen neuen IAM-Benutzer zu erstellen oder AWS Rechte zu ändern) von einer IP-

Adresse aus aufgerufen wurde, die in einer von Ihnen hochgeladenen Bedrohungsliste enthalten ist. In GuardDuty besteht eine Bedrohungsliste aus bekannten bösartigen IP-Adressen. Dies kann auf unbefugten Zugriff auf AWS Ressourcen in Ihrer Umgebung hinweisen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS

Anmeldeinformationen, die exklusiv für einen erstellt wurden AWS Amazon ECS-Aufgaben werden von einem anderen Konto aus verwendet AWS

Standard-Schweregrad: Hoch*

> **Note**
>
> Der Standard-Schweregrad diese Erkenntnis ist Hoch. Wenn die API jedoch von einem Konto aufgerufen wurde, das zu Ihrer AWS Umgebung gehört, ist der Schweregrad Mittel.

- Datenquelle: CloudTrail Verwaltungsereignisse oder CloudTrail Datenereignisse für S3

Dieses Ergebnis informiert Sie darüber, wenn Ihre AWS Amazon ECS-Aufgabenanmeldedaten verwendet werden, um APIs von einer IP-Adresse oder einem Amazon VPC-Endpunkt aus aufzurufen, der einem anderen AWS Konto gehört als dem, auf dem die zugehörige Ressource ausgeführt wird. Die VPC-Endpunkterkennung ist nur für Services verfügbar, die Netzwerkaktivitätsereignisse für VPC-Endpunkte unterstützen. Informationen zu Services, die Netzwerkaktivitätsereignisse für VPC-Endpunkte unterstützen, finden Sie im Benutzerhandbuch für AWS CloudTrail unter Protokollieren von Netzwerkaktivitätsereignissen.

AWS empfiehlt nicht, temporäre Anmeldeinformationen außerhalb der Entität weiterzuverteilen, die sie erstellt hat (z. B. AWS Anwendungen, Amazon EC2 oder Amazon Elastic Container Service). Autorisierte Benutzer können jedoch Anmeldeinformationen aus ihren Ressourcen exportieren, um legitime API-Aufrufe durchzuführen. Wenn das `remoteAccountDetails.affiliated` Feld aktiviert ist, bedeutet `True` dies, dass die API von einem Konto aufgerufen wurde, das demselben Administratorkonto zugeordnet ist. Um einen möglichen Angriff auszuschließen und die Legitimität

der Aktivität zu überprüfen, wenden Sie sich an den AWS-Konto Eigentümer oder IAM-Principal, dem diese Anmeldeinformationen zugewiesen sind.

> **Note**
>
> Wenn von einem Remote-Konto aus fortgesetzte Aktivitäten GuardDuty beobachtet werden, erkennt das Machine-Learning-Modell (ML) dies als erwartetes Verhalten. Daher GuardDuty wird dieses Ergebnis nicht mehr für Aktivitäten von diesem Remote-Konto aus generiert. GuardDuty wird weiterhin Erkenntnisse über neues Verhalten von anderen Remote-Konten generieren und erlernte Remote-Konten erneut bewerten, wenn sich das Verhalten im Laufe der Zeit ändert.

> **Note**
>
> Bei Amazon ECS-Aufgaben sind die Anmeldeinformationen der Aufgabenrolle zugeordnet, und die Erkennung erfolgt unabhängig von der VPC-Konfiguration.

Empfehlungen zur Abhilfe:

Dieses Ergebnis wird generiert, wenn AWS API-Anfragen innerhalb AWS einer Ressource außerhalb von Ihnen mithilfe Ihrer AWS-Konto AWS Amazon ECS-Aufgabenrolle gestellt werden. Es kann üblich sein, beispielsweise bei der Transit Gateway-Architektur in einer https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/transit-vpc-solution.html Hub-and-Spoke-Konfiguration, den Datenverkehr über eine einzelne Hub-VPC mit AWS Service-Endpunkten weiterzuleiten. Wenn dies ein erwartetes Verhalten ist, empfehlen wir, Unterdrückungsregeln zusammen mit den Filterkriterien den Findetyp zu verwenden, der UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS

Als Reaktion auf diese Erkenntnis können Sie den folgenden Workflow verwenden, um das weitere Vorgehen festzulegen:

1. Identifizieren Sie das betroffene Remote-Konto im Feld `service.action.awsApiCallAction.remoteAccountDetails.accountId`.
2. Stellen Sie vor `service.action.awsApiCallAction.remoteAccountDetails.affiliated` Ort fest, ob das Konto mit Ihrer GuardDuty Umgebung verknüpft ist.

3. Wenn das Konto verknüpft ist, wenden Sie sich an den Remote-Kontoinhaber und den Besitzer der Ressourcenanmeldedaten, um dies zu überprüfen.

   Wenn das Konto nicht verknüpft ist, müssen Sie zunächst prüfen, ob dieses Konto mit Ihrer Organisation verknüpft ist, aber nicht Teil Ihrer Umgebung mit GuardDuty mehreren Konten ist oder ob GuardDuty es in diesem Konto noch nicht aktiviert wurde. Wenden Sie sich als Nächstes an den Besitzer der Ressourcenanmeldedaten, um zu ermitteln, ob es einen Anwendungsfall für die Verwendung dieser Anmeldeinformationen durch ein Remote-Konto gibt.
4. Wenn der Eigentümer der Anmeldeinformationen das entfernte Konto nicht erkennt, wurden die Anmeldeinformationen möglicherweise von einem Bedrohungsakteur innerhalb von AWS kompromittiert. Sie sollten die unter empfohlenen Maßnahmen ergreifenBehebung eines potenziell kompromittierten ECS-Clusters, um Ihre Umgebung zu schützen.

   Darüber hinaus können Sie eine Missbrauchsmeldung an das AWS Trust and Safety-Team senden, um eine Untersuchung des Remote-Kontos einzuleiten. Wenn Sie Ihren Bericht an AWS Trust and Safety senden, geben Sie die vollständigen JSON-Details des Befundes an.

UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS

Anmeldeinformationen, die exklusiv für einen erstellt wurden AWS Ressourcen (eine Lambda-Funktion oder eine Amazon ECS-Aufgabe) werden von einer IP-Adresse außerhalb von verwendet AWS.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Verwaltungsereignisse oder CloudTrail Datenereignisse für S3

Dieses Ergebnis informiert Sie darüber, dass ein Host außerhalb von AWS versucht hat, AWS API-Operationen mit temporären AWS Anmeldeinformationen auszuführen, die für eine AWS Ressource (eine Lambda-Funktion oder Amazon ECS-Aufgabe) in Ihrer AWS Umgebung erstellt wurden. Die aufgeführte Ressource ist möglicherweise kompromittiert, und die temporären Anmeldeinformationen dieser Ressource wurden möglicherweise auf einen externen Host außerhalb von exfiltriert. AWS

AWS empfiehlt nicht, temporäre Anmeldeinformationen außerhalb der Entität weiterzuverteilen, die sie erstellt hat (z. B. AWS Anwendungen wie Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Service oder). AWS Lambda Autorisierte Benutzer können jedoch Anmeldeinformationen aus ihren Ressourcen exportieren, um legitime API-Aufrufe durchzuführen.

Um einen möglichen Angriff auszuschließen und die Legitimität der Aktivität zu überprüfen, überprüfen Sie, ob die Verwendung von Ressourcenanmeldeinformationen von der Remote-IP in dem Ergebnis zu erwarten ist.

> **Note**
>
> Wenn von einem Remote-Host aus fortgesetzte Aktivitäten GuardDuty beobachtet werden, erkennt das Machine-Learning-Modell (ML) dies als erwartetes Verhalten. Daher GuardDuty wird dieses Ergebnis nicht mehr für Aktivitäten von diesem Remote-Host generiert. GuardDuty generiert weiterhin Erkenntnisse über neues Verhalten von anderen Remote-Hosts und bewertet die gelernten Remote-Hosts erneut, wenn sich das Verhalten im Laufe der Zeit ändert.

Empfehlungen zur Abhilfe:

Diese Erkenntnis wird generiert, wenn das Netzwerk so konfiguriert ist, dass der Internetdatenverkehr von einem On-Premises-Gateway und nicht von einem VPC-Internet-Gateway (IGW) ausgeht. Geläufige Konfigurationen, z. B. die Verwendung von AWS Outposts oder VPC-VPN-Verbindungen, können dazu führen, dass Datenverkehr auf diese Weise weitergeleitet wird. Wenn dies ein erwartetes Verhalten ist, GuardDuty empfiehlt dann, Unterdrückungsregeln die Verwendung einer Regel mit zwei Filterkriterien zu verwenden. Das erste Kriterium ist der Erkenntnistyp, der `UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS` sein sollte. Das zweite Filterkriterium ist die IPv4-Adresse des API-Aufrufers mit der IP-Adresse oder dem CIDR-Bereich für Ihren On-Premises-Internet-Gateway.

Wenn solche Aktivitäten unerwartet auftreten, sind Ihre Anmeldeinformationen möglicherweise kompromittiert. Hinweise zu den Schritten zur Behebung dieses Befundtyps finden Sie unter oderBehebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten. Behebung eines potenziell kompromittierten ECS-Clusters

UnauthorizedAccess:IAMUser/TorIPCaller

Eine API wurde von einer IP-Adresse eines Tor-Ausgangsknotens aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Verwaltungsereignisse

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang (Beispiel: ein Versuch zum Starten einer EC2-Instance, Erstellen eines neuen IAM-Benutzers oder Ändern Ihrer AWS -Rechte) von einer IP-Adresse eines Tor-Ausgangsknotens aufgerufen wurde. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese nach dem Zufallsprinzip durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Dies kann auf einen unbefugten Zugriff auf Ihre AWS -Ressourcen hinweisen, mit dem Ziel, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

GuardDuty Arten der Suche nach Angriffssequenzen

GuardDuty erkennt eine Angriffssequenz, wenn eine bestimmte Abfolge mehrerer Aktionen mit einer potenziell verdächtigen Aktivität übereinstimmt. Eine Angriffssequenz umfasst Signale wie API-Aktivitäten und GuardDuty Ergebnisse. Wenn eine Gruppe von Signalen in einer bestimmten Reihenfolge GuardDuty beobachtet wird, die auf eine laufende, anhaltende oder kürzlich aufgetretene Sicherheitsbedrohung hindeuten, wird ein Ergebnis der Angriffssequenz GuardDuty generiert. GuardDuty betrachtet einzelne API-Aktivitäten soweak signals, als ob sie sich nicht als potenzielle Bedrohung darstellen.

Die Erkennungen der Angriffssequenz konzentrieren sich auf die potenzielle Gefährdung von Amazon S3 S3-Daten (die Teil eines umfassenderen Ransomware-Angriffs sein können), kompromittierte AWS Anmeldeinformationen, kompromittierte Amazon EKS-Cluster, kompromittierte Amazon ECS-Cluster und kompromittierte Amazon EC2 EC2-Instanzgruppen. Die folgenden Abschnitte enthalten Einzelheiten zu den einzelnen Angriffssequenzen.

Themen

- AttackSequence:EKS/CompromisedCluster
- AttackSequence:ECS/CompromisedCluster
- AttackSequence:EC2/CompromisedInstanceGroup
- AttackSequence:IAM/CompromisedCredentials
- AttackSequence:S3/CompromisedData

AttackSequence:EKS/CompromisedCluster

Eine Abfolge verdächtiger Aktionen, die von einem potenziell kompromittierten Amazon EKS-Cluster ausgeführt werden.

- Standardschweregrad: Kritisch
- Datenquellen:
  - EKS-Auditprotokollereignisse
  - Laufzeitüberwachung für Amazon EKS
  - Amazon EKS-Malware-Erkennung für Amazon EC2
  - AWS CloudTrail Datenereignisse für S3
  - AWS CloudTrail Verwaltungsereignisse
  - VPC Flow Logs
  - Route53 Resolver DNS-Abfrageprotokolle

Dieses Ergebnis informiert Sie darüber, dass Sie eine Abfolge verdächtiger Aktionen GuardDuty entdeckt haben, die auf einen potenziell gefährdeten Amazon EKS-Cluster in Ihrer Umgebung hindeuten. In demselben Amazon EKS-Cluster wurden mehrere verdächtige und anomale Angriffsverhalten beobachtet, z. B. bösartige Prozesse oder Verbindungen mit böswilligen Endpunkten.

GuardDuty verwendet seine eigenen Korrelationsalgorithmen, um die Reihenfolge der Aktionen zu beobachten und zu identifizieren, die mithilfe der IAM-Anmeldeinformationen ausgeführt werden. GuardDuty bewertet die Ergebnisse anhand von Schutzplänen und anderen Signalquellen, um gängige und sich abzeichnende Angriffsmuster zu identifizieren. GuardDuty nutzt mehrere Faktoren, um Bedrohungen aufzudecken, wie z. B. IP-Reputation, API-Sequenzen, Benutzerkonfiguration und potenziell betroffene Ressourcen.

Behebungsmaßnahmen: Wenn dieses Verhalten in Ihrer Umgebung unerwartet auftritt, ist Ihr Amazon EKS-Cluster möglicherweise gefährdet. Umfassende Anleitungen zur Problembehebung finden Sie unter und. Behebung der EKS-Schutzfeststellungen Korrigieren von Erkenntnissen der Laufzeitüberwachung

Da AWS Anmeldeinformationen möglicherweise durch den EKS-Cluster kompromittiert wurden, finden Sie außerdem weitere Informationen unter. Behebung potenziell kompromittierter

Bedrohungen AWS Anmeldedaten Schritte zur Behebung anderer Ressourcen, die möglicherweise betroffen waren, finden Sie unter. Behebung erkannter GuardDuty Sicherheitslücken

AttackSequence:ECS/CompromisedCluster

Eine Abfolge verdächtiger Aktionen, die von einem potenziell kompromittierten Amazon ECS-Cluster ausgeführt werden.

- Standardschweregrad: Kritisch
- Datenquellen:
  - Laufzeitüberwachung für Amazon ECS Fargate
  - Laufzeitüberwachung für EC2-Instances in Amazon ECS
  - GuardDuty Malware-Schutz für Amazon EC2

Dieser Befund informiert Sie darüber, dass eine Folge verdächtiger Signale GuardDuty erkannt wurde, die auf einen potenziell gefährdeten Amazon ECS-Cluster in Ihrer Umgebung hinweisen. Zu diesen Signalen können bösartige Prozesse, Kommunikation mit böswilligen Endpunkten oder Verhalten beim Cryptocurrency Mining gehören.

GuardDuty verwendet firmeneigene Korrelationsalgorithmen und mehrere Erkennungsfaktoren, um Sequenzen verdächtiger Aktionen innerhalb von Amazon ECS-Clustern zu identifizieren. Durch die Analyse verschiedener Schutzpläne und verschiedener Signalquellen GuardDuty werden häufig auftretende und neu entstehende Angriffsmuster identifiziert, sodass potenzielle Sicherheitslücken mit hoher Zuverlässigkeit erkannt werden können.

Abhilfemaßnahmen: Wenn dieses Verhalten in Ihrer Umgebung unerwartet auftritt, ist Ihr Amazon ECS-Cluster möglicherweise gefährdet. Empfehlungen zur Eindämmung von Bedrohungen finden Sie unter. Behebung eines potenziell kompromittierten ECS-Clusters Beachten Sie, dass sich die Gefährdung auf eine oder mehrere ECS-Tasks oder Container-Workloads erstrecken kann, die zur Erstellung oder Änderung AWS von Ressourcen hätten verwendet werden können. Umfassende Hinweise zur Problembehebung für potenziell betroffene Ressourcen finden Sie unter. Behebung erkannter GuardDuty Sicherheitslücken

AttackSequence:EC2/CompromisedInstanceGroup

Eine Abfolge verdächtiger Aktionen, die auf potenziell gefährdete Amazon EC2 EC2-Instances hinweisen.

- Standardschweregrad: Kritisch
- Datenquellen:
  - Laufzeitüberwachung für Amazon EC2
  - Malware-Erkennung für Amazon EC2
  - VPC Flow Logs
  - Route53 Resolver DNS-Abfrageprotokolle

Dieses Ergebnis deutet darauf hin, dass eine Abfolge verdächtiger Aktionen GuardDuty erkannt wurde, die auf eine potenzielle Gefährdung einer Gruppe von Amazon EC2 EC2-Instances in Ihrer Umgebung hindeuten. Instanzgruppen stellen in der Regel Anwendungen dar, die über Infrastructure-as-Code verwaltet werden und ähnliche Konfigurationen wie Auto-scaling Gruppe, IAM-Instance-Profilrolle, AWS CloudFormation Stack, Amazon EC2 EC2-Startvorlage, AMI oder VPC-ID gemeinsam nutzen. GuardDuty beobachtete mehrere verdächtige Verhaltensweisen in einer oder mehreren Instances, darunter:

- Bösartige Prozesse
- Bösartige Dateien
- Verdächtige Netzwerkverbindungen
- Mining-Aktivitäten für Kryptowährungen
- Verdächtige Verwendung von Amazon EC2 EC2-Instance-Anmeldeinformationen

Erkennungsmethode: GuardDuty verwendet firmeneigene Korrelationsalgorithmen, um verdächtige Aktionssequenzen innerhalb von Amazon EC2 EC2-Instances zu identifizieren. Durch die Auswertung der Ergebnisse anhand verschiedener Schutzpläne und verschiedener Signalquellen GuardDuty werden Angriffsmuster anhand mehrerer Faktoren wie IP- und Domain-Reputation sowie verdächtiger laufender Prozesse identifiziert.

Abhilfemaßnahmen: Wenn dieses Verhalten in Ihrer Umgebung unerwartet auftritt, sind Ihre Amazon EC2 EC2-Instances möglicherweise gefährdet. Der Kompromiss könnte Folgendes beinhalten:

- Mehrere Prozesse
- Instance-Anmeldeinformationen, die möglicherweise zur Änderung von Amazon EC2 EC2-Instances oder anderen AWS Ressourcen verwendet wurden

Empfehlungen zur Eindämmung von Bedrohungen finden Sie unter. Behebung einer potenziell kompromittierten Amazon EC2-Instance Beachten Sie, dass sich die Kompromittierung auf eine oder mehrere Amazon EC2 EC2-Instances erstrecken kann und kompromittierte Prozesse oder Instance-Anmeldeinformationen beinhalten kann, die zur Erstellung oder Änderung von Amazon EC2 EC2-Instances oder anderen Ressourcen hätten verwendet werden können. AWS Umfassende Hinweise zur Problembehebung für potenziell betroffene Ressourcen finden Sie unter. Behebung erkannter GuardDuty Sicherheitslücken

AttackSequence:IAM/CompromisedCredentials

Eine Abfolge von API-Anfragen, die mithilfe potenziell kompromittierter Anmeldeinformationen aufgerufen wurden. AWS

- Standardschweregrad: Kritisch
- Datenquelle: AWS CloudTrail Verwaltungsereignisse

Dieses Ergebnis informiert Sie darüber, dass Sie eine Folge verdächtiger Aktionen GuardDuty entdeckt haben, die mithilfe von AWS Anmeldeinformationen ausgeführt wurden und sich auf eine oder mehrere Ressourcen in Ihrer Umgebung auswirken. Mit denselben Anmeldeinformationen wurden mehrere verdächtige und anomale Angriffsverhaltensweisen beobachtet, was zu einer höheren Wahrscheinlichkeit führte, dass die Anmeldeinformationen missbraucht wurden.

GuardDuty verwendet seine firmeneigenen Korrelationsalgorithmen, um die Reihenfolge der Aktionen zu beobachten und zu identifizieren, die mithilfe der IAM-Anmeldeinformationen ausgeführt wurden. GuardDuty bewertet die Ergebnisse anhand von Schutzplänen und anderen Signalquellen, um gängige und sich abzeichnende Angriffsmuster zu identifizieren. GuardDuty nutzt mehrere Faktoren, um Bedrohungen aufzudecken, wie z. B. IP-Reputation, API-Sequenzen, Benutzerkonfiguration und potenziell betroffene Ressourcen.

Behebungsmaßnahmen: Wenn dieses Verhalten in Ihrer Umgebung unerwartet auftritt, wurden Ihre AWS Anmeldeinformationen möglicherweise kompromittiert. Schritte zur Problembehebung finden Sie unter. Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten Die kompromittierten Anmeldeinformationen wurden möglicherweise verwendet, um zusätzliche

Ressourcen wie Amazon S3-Buckets, AWS Lambda Funktionen oder Amazon EC2 EC2-Instances in Ihrer Umgebung zu erstellen oder zu ändern. Schritte zur Behebung anderer Ressourcen, die möglicherweise beeinträchtigt wurden, finden Sie unter. Behebung erkannter GuardDuty Sicherheitslücken

AttackSequence:S3/CompromisedData

Bei einem möglichen Versuch, Daten in Amazon S3 zu exfiltrieren oder zu vernichten, wurde eine Abfolge von API-Anfragen aufgerufen.

- Standardschweregrad: Kritisch
- Datenquellen: AWS CloudTrail Datenereignisse für S3 und AWS CloudTrail Verwaltungsereignisse

Dieses Ergebnis informiert Sie darüber, dass Sie in einem oder mehreren Amazon Simple Storage Service (Amazon S3) -Buckets eine Abfolge verdächtiger Aktionen GuardDuty entdeckt haben, die auf eine Datenkompromittierung hindeuten. Dabei wurden potenziell AWS kompromittierte Anmeldeinformationen verwendet. Es wurden mehrere verdächtige und ungewöhnliche Angriffsverhaltensweisen (API-Anfragen) beobachtet, was dazu führte, dass die Wahrscheinlichkeit, dass die Anmeldeinformationen missbraucht werden, höher war.

GuardDuty verwendet seine Korrelationsalgorithmen, um die Reihenfolge der Aktionen zu beobachten und zu identifizieren, die mithilfe der IAM-Anmeldeinformationen ausgeführt wurden. GuardDuty bewertet dann die Ergebnisse anhand von Schutzplänen und anderen Signalquellen, um gängige und sich abzeichnende Angriffsmuster zu identifizieren. GuardDuty nutzt mehrere Faktoren, um Bedrohungen aufzudecken, z. B. IP-Reputation, API-Sequenzen, Benutzerkonfiguration und potenziell betroffene Ressourcen.

Abhilfemaßnahmen: Wenn diese Aktivität in Ihrer Umgebung unerwartet auftritt, wurden Ihre AWS Anmeldeinformationen oder Amazon S3 S3-Daten möglicherweise exfiltriert oder zerstört. Schritte zur Problembehebung finden Sie unter und. Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten Behebung eines potenziell kompromittierten S3-Buckets

GuardDuty S3 Schutzsuchtypen

Die folgenden Ergebnisse beziehen sich spezifisch auf Amazon S3-Ressourcen und geben als Ressourcentyp an, `S3Bucket` ob es sich bei der Datenquelle um CloudTrail Datenereignisse für S3 handelt oder `AccessKey` ob es sich bei der Datenquelle um CloudTrail Verwaltungsereignisse

handelt. Der Schweregrad und die Details der Ergebnisse unterscheiden sich je nach Ergebnistyp und Berechtigung, die dem Bucket zugeordnet sind.

Die hier aufgeführten Erkenntnisse beinhalten die Datenquellen und Modelle, die zur Generierung dieses Erkenntnistyps verwendet wurden. Weitere Informationen zu Datenquellen und Modellen finden Sie unter GuardDuty grundlegende Datenquellen.

> **Important**
>
> Ergebnisse mit einer Datenquelle von CloudTrail Datenereignissen für S3 werden nur generiert, wenn Sie S3 Protection aktiviert haben. Nach dem 31. Juli 2020 ist S3 Protection standardmäßig aktiviert, wenn ein Konto GuardDuty zum ersten Mal aktiviert wird oder wenn ein delegiertes GuardDuty Administratorkonto GuardDuty in einem vorhandenen Mitgliedskonto aktiviert wird. Wenn jedoch ein neues Mitglied der GuardDuty Organisation beitritt, gelten die Einstellungen der Organisation für die automatische Aktivierung. Informationen zu Einstellungen für die automatische Aktivierung finden Sie unter. Einstellungen für die automatische Aktivierung von Organisationen festlegen Informationen zur Aktivierung des S3-Schutzes finden Sie unter GuardDuty S3-Schutz

Für alle `S3Bucket`-Arten von Erkenntnissen wird empfohlen, die Berechtigungen für den betreffenden Bucket und die Berechtigungen aller Benutzer, die an dem Erkenntniss beteiligt waren, zu überprüfen. Falls die Aktivität unerwartet ist, lesen Sie die Empfehlungen zur Problembehebung unter Behebung eines potenziell kompromittierten S3-Buckets.

Themen

- Discovery:S3/AnomalousBehavior
- Discovery:S3/MaliciousIPCaller
- Discovery:S3/MaliciousIPCaller.Custom
- Discovery:S3/TorIPCaller
- Exfiltration:S3/AnomalousBehavior
- Exfiltration:S3/MaliciousIPCaller
- Impact:S3/AnomalousBehavior.Delete
- Impact:S3/AnomalousBehavior.Permission
- Impact:S3/AnomalousBehavior.Write

- Impact:S3/MaliciousIPCaller
- PenTest:S3/KaliLinux
- PenTest:S3/ParrotLinux
- PenTest:S3/PentooLinux
- Policy:S3/AccountBlockPublicAccessDisabled
- Policy:S3/BucketAnonymousAccessGranted
- Policy:S3/BucketBlockPublicAccessDisabled
- Policy:S3/BucketPublicAccessGranted
- Stealth:S3/ServerAccessLoggingDisabled
- UnauthorizedAccess:S3/MaliciousIPCaller.Custom
- UnauthorizedAccess:S3/TorIPCaller

Discovery:S3/AnomalousBehavior

Eine API, die häufig zum Auffinden von S3-Objekten verwendet wird, wurde auf ungewöhnliche Weise aufgerufen.

Standard-Schweregrad: Niedrig

- Datenquelle: CloudTrail Datenereignisse für S3

Diese Erkenntnis informiert Sie darüber, dass eine IAM-Entität eine S3-API aufgerufen hat, um S3-Buckets in Ihrer Umgebung zu erkennen, z. B. `ListObjects`. Diese Art von Aktivität ist mit der Erkennungsphase eines Angriffs verbunden, in der ein Angreifer Informationen sammelt, um festzustellen, ob Ihre AWS Umgebung für einen umfassenderen Angriff anfällig ist. Diese Aktivität ist verdächtig, da die Art und Weise, wie die IAM-Entität die API aufgerufen hat, ungewöhnlich war. Beispielsweise ruft eine IAM-Entität ohne vorherige Historie eine S3-API auf, oder eine IAM-Entität ruft eine S3-API von einem ungewöhnlichen Ort aus auf.

Diese API wurde durch das Modell GuardDuty des maschinellen Lernens (ML) zur Erkennung von Anomalien als anomal identifiziert. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Techniken von Angreifern in Verbindung gebracht werden. Es verfolgt verschiedene Faktoren der API-Anfragen, wie z. B. den Nutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, die spezifische API, die angefordert wurde,

den angeforderten Bucket und die Anzahl der durchgeführten API-Aufrufe. Weitere Informationen darüber, welche Faktoren der API-Anforderung für die Benutzeridentität, die die Anforderung aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten S3-Buckets.

Discovery:S3/MaliciousIPCaller

Eine S3-API, die häufig zum Auffinden von Ressourcen in einem verwendet wird AWS Die Umgebung wurde von einer bekannten bösartigen IP-Adresse aus aufgerufen.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Datenereignisse für S3

Diese Erkenntnis informiert Sie darüber, dass ein S3-API-Vorgang von einer IP-Adresse aus aufgerufen wurde, die mit bekannten böswilligen Aktivitäten in Verbindung steht. Die beobachtete API wird häufig mit der Erkennungsphase eines Angriffs in Verbindung gebracht, in der ein Gegner Informationen über Ihre AWS Umgebung sammelt. Beispiele hierfür sind `GetObjectAcl` und `ListObjects`.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten S3-Buckets.

Discovery:S3/MaliciousIPCaller.Custom

Eine S3-API wurde von einer IP-Adresse aufgerufen, die sich auf einer benutzerdefinierten Bedrohungsliste befindet.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Datenereignisse für S3

Diese Erkenntnis informiert Sie darüber, dass eine S3-API, wie z. B. `GetObjectAcl` oder `ListObjects` von einer IP-Adresse aufgerufen wurde, die auf einer von Ihnen hochgeladenen Bedrohungsliste steht. Die mit dieser Erkenntnis verknüpfte Bedrohungsliste ist im Abschnitt Zusätzliche Informationen der Details zu einer Erkenntnis aufgeführt. Die beobachtete API wird häufig mit der Erkennungsphase eines Angriffs in Verbindung gebracht, in der ein Angreifer Informationen sammelt, um festzustellen, ob Ihre AWS -Umgebung für einen umfassenderen Angriff anfällig ist.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten S3-Buckets.

Discovery:S3/TorIPCaller

Eine S3-API wurde von einer Tor-Ausgangsknotens-IP-Adresse aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Datenereignisse für S3

Diese Erkenntnis informiert Sie darüber, dass eine S3-API, wie `GetObjectAcl` oder`ListObjects`, von einer IP-Adresse des Tor-Ausgangsknotens aus aufgerufen wurde. Diese Art von Aktivität ist mit der Erkennungsphase eines Angriffs verbunden, in der ein Angreifer Informationen sammelt, um festzustellen, ob Ihre AWS Umgebung für einen umfassenderen Angriff anfällig ist. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese nach dem Zufallsprinzip durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Dies kann auf einen unbefugten Zugriff auf Ihre AWS Ressourcen hinweisen, mit der Absicht, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten S3-Buckets.

Exfiltration:S3/AnomalousBehavior

Eine IAM-Entität hat eine S3-API auf verdächtige Weise aufgerufen.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Datenereignisse für S3

Diese Erkenntnis informiert Sie darüber, dass eine IAM-Entität API-Aufrufe tätigt, die einen S3-Bucket betreffen, und dass sich diese Aktivität von der festgelegten Basisaktivität dieser Entität unterscheidet. Der in dieser Aktivität verwendete API-Aufruf steht im Zusammenhang mit der Exfiltrationsphase eines Angriffs, in der ein Angreifer versucht, Daten zu sammeln. Diese Aktivität ist verdächtig, da die Art und Weise, wie die IAM-Entität die API aufgerufen hat, ungewöhnlich war. Beispielsweise ruft eine IAM-Entität ohne vorherige Historie eine S3-API auf, oder eine IAM-Entität ruft eine S3-API von einem ungewöhnlichen Ort aus auf.

Diese API wurde durch das Modell GuardDuty des maschinellen Lernens (ML) zur Erkennung von Anomalien als anomal identifiziert. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Techniken von Angreifern in Verbindung gebracht werden. Es verfolgt verschiedene Faktoren der API-Anfragen, wie z. B. den Nutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, die spezifische API, die angefordert wurde, den angeforderten Bucket und die Anzahl der durchgeführten API-Aufrufe. Weitere Informationen darüber, welche Faktoren der API-Anforderung für die Benutzeridentität, die die Anforderung aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten S3-Buckets.

Exfiltration:S3/MaliciousIPCaller

Eine S3-API, die häufig zum Sammeln von Daten von einem verwendet wird AWS Die Umgebung wurde von einer bekannten bösartigen IP-Adresse aus aufgerufen.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Datenereignisse für S3

Diese Erkenntnis informiert Sie darüber, dass ein S3-API-Vorgang von einer IP-Adresse aus aufgerufen wurde, die mit bekannten böswilligen Aktivitäten in Verbindung steht. Die beobachtete API wird häufig mit Exfiltrationstaktiken in Verbindung gebracht, bei denen ein Angreifer versucht, Daten aus Ihrem Netzwerk zu sammeln. Beispiele hierfür sind `GetObject` und `CopyObject`.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten S3-Buckets.

Impact:S3/AnomalousBehavior.Delete

Eine IAM-Entität hat eine S3-API aufgerufen, die versucht, Daten auf verdächtige Weise zu löschen.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Datenereignisse für S3

Dieses Ergebnis informiert Sie darüber, dass eine IAM-Entität in Ihrer AWS Umgebung API-Aufrufe tätigt, die einen S3-Bucket beinhalten, und dieses Verhalten unterscheidet sich von der etablierten Basislinie dieser Entität. Der in dieser Aktivität verwendete API-Aufruf steht im Zusammenhang mit einem Angriff, bei dem versucht wird, Daten zu löschen. Diese Aktivität ist verdächtig, da die Art und Weise, wie die IAM-Entität die API aufgerufen hat, ungewöhnlich war. Beispielsweise ruft eine IAM-Entität ohne vorherige Historie eine S3-API auf, oder eine IAM-Entität ruft eine S3-API von einem ungewöhnlichen Ort aus auf.

Diese API wurde durch das Modell GuardDuty des maschinellen Lernens (ML) zur Erkennung von Anomalien als anomal identifiziert. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Techniken von Angreifern in Verbindung gebracht werden. Es verfolgt verschiedene Faktoren der API-Anfragen, wie z. B. den Nutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, die spezifische API, die angefordert wurde, den angeforderten Bucket und die Anzahl der durchgeführten API-Aufrufe. Weitere Informationen

darüber, welche Faktoren der API-Anforderung für die Benutzeridentität, die die Anforderung aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten S3-Buckets.

Wir empfehlen eine Prüfung des Inhalts Ihres S3-Buckets, um festzustellen, ob die vorherige Objektversion wiederhergestellt werden kann oder sollte.

Impact:S3/AnomalousBehavior.Permission

Eine API, die häufig zum Festlegen der Berechtigungen für Zugriffssteuerungslisten (ACL) verwendet wird, wurde auf ungewöhnliche Weise aufgerufen.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Datenereignisse für S3

Dieses Ergebnis informiert Sie darüber, dass eine IAM-Entität in Ihrer AWS Umgebung eine Bucket-Richtlinie oder ACL für die aufgelisteten S3-Buckets aktualisiert hat. Diese Änderung kann Ihre S3-Buckets allen authentifizierten Benutzern öffentlich zugänglich machen. AWS

Diese API wurde durch das Modell GuardDuty des maschinellen Lernens (ML) zur Erkennung von Anomalien als anomal identifiziert. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Techniken von Angreifern in Verbindung gebracht werden. Es verfolgt verschiedene Faktoren der API-Anfragen, wie z. B. den Nutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, die spezifische API, die angefordert wurde, den angeforderten Bucket und die Anzahl der durchgeführten API-Aufrufe. Weitere Informationen darüber, welche Faktoren der API-Anforderung für die Benutzeridentität, die die Anforderung aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv

genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten S3-Buckets.

Wir empfehlen eine Prüfung des Inhalts Ihres S3-Buckets, um sicherzustellen, dass kein unerwarteter öffentlicher Zugriff auf Objekte gewährt wurde.

Impact:S3/AnomalousBehavior.Write

Eine IAM-Entität hat eine S3-API aufgerufen, die versucht, Daten auf verdächtige Weise zu schreiben.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Datenereignisse für S3

Dieses Ergebnis informiert Sie darüber, dass eine IAM-Entität in Ihrer AWS Umgebung API-Aufrufe tätigt, die einen S3-Bucket beinhalten, und dieses Verhalten unterscheidet sich von der etablierten Basislinie dieser Entität. Der in dieser Aktivität verwendete API-Aufruf steht im Zusammenhang mit einem Angriff, bei dem versucht wird, Daten zu schreiben. Diese Aktivität ist verdächtig, da die Art und Weise, wie die IAM-Entität die API aufgerufen hat, ungewöhnlich war. Beispielsweise ruft eine IAM-Entität ohne vorherige Historie eine S3-API auf, oder eine IAM-Entität ruft eine S3-API von einem ungewöhnlichen Ort aus auf.

Diese API wurde durch das Modell GuardDuty des maschinellen Lernens (ML) zur Erkennung von Anomalien als anomal identifiziert. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Techniken von Angreifern in Verbindung gebracht werden. Es verfolgt verschiedene Faktoren der API-Anfragen, wie z. B. den Nutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, die spezifische API, die angefordert wurde, den angeforderten Bucket und die Anzahl der durchgeführten API-Aufrufe. Weitere Informationen darüber, welche Faktoren der API-Anforderung für die Benutzeridentität, die die Anforderung aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten S3-Buckets.

Wir empfehlen eine Prüfung des Inhalts Ihres S3-Buckets, um sicherzustellen, dass bei diesem API-Aufruf keine schädlichen oder unautorisierten Daten geschrieben wurden.

Impact:S3/MaliciousIPCaller

Eine S3-API, die häufig zur Manipulation von Daten oder Prozessen in einem verwendet wird AWS Die Umgebung wurde von einer bekannten bösartigen IP-Adresse aus aufgerufen.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Datenereignisse für S3

Diese Erkenntnis informiert Sie darüber, dass ein S3-API-Vorgang von einer IP-Adresse aus aufgerufen wurde, die mit bekannten böswilligen Aktivitäten in Verbindung steht. Die beobachtete API wird häufig mit Impact-Taktiken in Verbindung gebracht, bei denen ein Gegner versucht, Daten in Ihrer Umgebung zu manipulieren, zu unterbrechen oder zu zerstören. AWS Beispiele hierfür sind `PutObject` und `PutObjectAcl`.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten S3-Buckets.

PenTest:S3/KaliLinux

Eine S3-API wurde von einem Kali-Linux-Computer aus aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: Datenereignisse für S3 CloudTrail

Dieses Ergebnis informiert Sie darüber, dass ein Computer, auf dem Kali Linux ausgeführt wird, S3-API-Aufrufe mit Anmeldeinformationen durchführt, die zu Ihrem AWS Konto gehören. Ihre Anmeldeinformationen wurden möglicherweise kompromittiert. Kali Linux ist ein beliebtes Tool für Penetrationstests, das von Sicherheitsexperten verwendet wird, um Schwachstellen in EC2-

Instances zu erkennen, für die Patches erforderlich sind. Angreifer verwenden dieses Tool auch, um Sicherheitslücken in der EC2-Konfiguration zu finden und sich unbefugten Zugriff auf Ihre AWS Umgebung zu verschaffen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten S3-Buckets.

PenTest:S3/ParrotLinux

Eine S3-API wurde von einem Computer mit Parrot Security Linux aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Datenereignisse für S3

Dieses Ergebnis informiert Sie darüber, dass ein Computer, auf dem Parrot Security Linux ausgeführt wird, S3-API-Aufrufe mit Anmeldeinformationen durchführt, die zu Ihrem AWS Konto gehören. Ihre Anmeldeinformationen wurden möglicherweise kompromittiert. Parrot Security Linux ist ein beliebtes Tool für Penetrationstests, das von Sicherheitsexperten verwendet wird, um Schwachstellen in EC2-Instances zu erkennen, für die Patches erforderlich sind. Dieses Tool wird allerdings auch von Angreifern verwendet, um Schwächen in der EC2-Konfiguration zu finden und nicht autorisierten Zugriff auf Ihre AWS -Umgebung zu erhalten.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten S3-Buckets.

PenTest:S3/PentooLinux

Eine S3-API wurde von einem Pentoo-Linux-Computer aus aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Datenereignisse für S3

Dieses Ergebnis informiert Sie darüber, dass ein Computer, auf dem Pentoo Linux ausgeführt wird, S3-API-Aufrufe mit Anmeldeinformationen durchführt, die zu Ihrem AWS Konto gehören. Ihre Anmeldeinformationen wurden möglicherweise kompromittiert. Pentoo Linux ist ein beliebtes Tool für Penetrationstests, das von Sicherheitsexperten verwendet wird, um Schwachstellen in EC2-Instances zu erkennen, für die Patches erforderlich sind. Angreifer nutzen dieses Tool auch, um Schwachstellen in der EC2-Konfiguration ausfindig zu machen und sich unbefugten Zugriff auf Ihre AWS Umgebung zu verschaffen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten S3-Buckets.

Policy:S3/AccountBlockPublicAccessDisabled

Eine IAM-Entität hat eine API aufgerufen, die verwendet wird, um Amazon S3 Block Public Access auf einen Bucket zu deaktivieren.

Standard-Schweregrad: Niedrig

- Datenquelle: CloudTrail Verwaltungsereignisse

Diese Erkenntnis informiert Sie darüber, dass Amazon S3 Block Public Access auf Kontoebene deaktiviert wurde. Wenn S3 Block Public Access aktiviert ist, werden entsprechende Einstellungen verwendet, um die auf den Bucket angewendeten Richtlinien oder Zugriffssteuerungslisten (ACL) zu filtern, um eine unbeabsichtigte öffentliche Offenlegung von Daten zu verhindern.

In der Regel ist S3 Block Public Access deaktiviert, um den öffentlichen Zugriff auf einen Bucket oder die Objekte im Bucket zuzulassen. Wenn S3 Block Public Access für ein Konto deaktiviert ist, wird der Zugriff auf Ihre Buckets durch die Richtlinien, ACLs oder Einstellungen von Block Public Access auf Bucket-Ebene gesteuert, die für Ihre individuellen Buckets gelten. Dies bedeutet nicht, dass der Bucket öffentlich freigegeben ist. Sie sollten die auf den Bucket angewendeten Berechtigungen jedoch überprüfen, um sicherzustellen, dass die passenden Zugangsebenen angewendet werden.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten S3-Buckets.

Policy:S3/BucketAnonymousAccessGranted

Ein IAM-Prinzipal hat den Zugriff auf einen S3-Bucket auf das Internet gewährt, indem er Bucket-Richtlinien oder ACLs geändert hat.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Verwaltungsereignisse

Diese Erkenntnis informiert Sie darüber, dass der aufgelistete S3-Bucket im Internet öffentlich zugänglich gemacht wurde, weil eine IAM-Entität eine Bucket-Richtlinie oder ACL für diesen Bucket geändert hat.

Nachdem eine Richtlinie- oder ACL-Änderung erkannt wurde, wird GuardDuty mithilfe automatisierter, von Zelkova unterstützter Argumentation ermittelt, ob der Bucket öffentlich zugänglich ist.

> **Note**
>
> Wenn die ACLs oder Bucket-Richtlinien eines Buckets so konfiguriert sind, dass sie explizit oder alles verweigern, spiegelt diese Erkenntnis möglicherweise nicht den aktuellen Status des Buckets wider. Diese Erkenntnis spiegelt nicht die Einstellungen für den öffentlichen Zugriff in S3, die möglicherweise für Ihren S3-Bucket aktiviert wurden, wider. In solchen Fällen wird der `effectivePermission`-Wert im Ergebnis als `UNKNOWN` markiert.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten S3-Buckets.

Policy:S3/BucketBlockPublicAccessDisabled

Ein IAM-Prinzipal hat eine API aufgerufen, die verwendet wird, um S3 Block Public Access auf einen Bucket zu deaktivieren.

Standard-Schweregrad: Niedrig

- Datenquelle: Ereignisse des Managements CloudTrail

Diese Erkenntnis informiert Sie darüber, dass Block Public Access für den S3-Bucket deaktiviert wurde. Wenn S3 Block Public Access aktiviert ist, werden entsprechende Einstellungen verwendet, um die auf den Bucket angewendeten Richtlinien oder Zugriffssteuerungslisten (ACL) zu filtern, um eine unbeabsichtigte öffentliche Offenlegung von Daten zu verhindern.

In der Regel ist S3 Block Public Access deaktiviert, um den öffentlichen Zugriff auf einen Bucket oder die Objekte im Bucket zuzulassen. Wenn S3 Block Public Access für diesen Bucket deaktiviert ist, wird der Zugriff auf den Bucket durch Richtlinien oder ACLs, gesteuert, die auf den Bucket angewendet sind. Dies bedeutet nicht, dass der Bucket öffentlich freigegeben ist. Sie sollten die auf den Bucket angewendeten Richtlinien und ACLs jedoch überprüfen, um sicherzustellen, dass die passenden Berechtigungen angewendet werden.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten S3-Buckets.

Policy:S3/BucketPublicAccessGranted

Ein IAM-Prinzipal hat allen öffentlichen Zugriff auf einen S3-Bucket gewährt AWS Benutzer, indem sie Bucket-Richtlinien oder ACLs ändern.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Verwaltungsereignisse

Dieses Ergebnis informiert Sie darüber, dass der aufgelistete S3-Bucket allen authentifizierten AWS Benutzern öffentlich zugänglich gemacht wurde, weil eine IAM-Entität eine Bucket-Richtlinie oder ACL für diesen S3-Bucket geändert hat.

Nachdem eine Richtlinie- oder ACL-Änderung erkannt wurde, wird mithilfe von Zelkova automatisiertes Reasoning GuardDuty verwendet, um festzustellen, ob der Bucket öffentlich zugänglich ist.

> **Note**
>
> Wenn die ACLs oder Bucket-Richtlinien eines Buckets so konfiguriert sind, dass sie explizit oder alles verweigern, spiegelt diese Erkenntnis möglicherweise nicht den aktuellen Status des Buckets wider. Diese Erkenntnis spiegelt nicht die Einstellungen für den öffentlichen Zugriff in S3, die möglicherweise für Ihren S3-Bucket aktiviert wurden, wider. In solchen Fällen wird der `effectivePermission`-Wert im Ergebnis als `UNKNOWN` markiert.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten S3-Buckets.

Stealth:S3/ServerAccessLoggingDisabled

S3-Server-Zugriffsprotokollierung für einen Bucket wurde deaktiviert.

Standard-Schweregrad: Niedrig

- Datenquelle: Ereignisse des Managements CloudTrail

Dieses Ergebnis informiert Sie darüber, dass die S3-Serverzugriffsprotokollierung für einen Bucket in Ihrer AWS Umgebung deaktiviert ist. Wenn diese Option deaktiviert ist, werden keine Webanforderungsprotokolle für Versuche erstellt, auf den identifizierten S3-Bucket zuzugreifen. S3-Verwaltungs-API-Aufrufe an den Bucket, z. B. DeleteBucket, werden jedoch weiterhin verfolgt. Wenn die S3-Datenereignisprotokollierung CloudTrail für diesen Bucket aktiviert ist, werden Webanfragen für Objekte innerhalb des Buckets weiterhin verfolgt. Das Deaktivieren der Protokollierung ist eine

Methode, die häufig von nicht autorisierten Benutzern verwendet wird, um ihre Spuren zu verwischen. Weitere Informationen zu S3-Protokollen finden Sie unter S3-Serverzugriffsprotokollierung und Optionen für S3-Protokollierung.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten S3-Buckets.

UnauthorizedAccess:S3/MaliciousIPCaller.Custom

Eine S3-API wurde von einer IP-Adresse aufgerufen, die sich auf einer benutzerdefinierten Bedrohungsliste befindet.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Datenereignisse für S3

Diese Erkenntnis informiert Sie darüber, dass ein S3-API-Vorgang, z. B. `PutObject` oder `PutObjectAcl`, von einer IP-Adresse aufgerufen wurde, die auf einer von Ihnen hochgeladenen Bedrohungsliste steht. Die mit dieser Erkenntnis verknüpfte Bedrohungsliste ist im Abschnitt Zusätzliche Informationen der Details zu einer Erkenntnis aufgeführt.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten S3-Buckets.

UnauthorizedAccess:S3/TorIPCaller

Eine S3-API wurde von einer Tor-Ausgangsknotens-IP-Adresse aufgerufen.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Datenereignisse für S3

Diese Erkenntnis informiert Sie darüber, dass ein S3-API-Vorgang, wie zum Beispiel `PutObject` oder `PutObjectAcl`, von einer IP-Adresse eines Tor-Ausgangsknotens aus aufgerufen wurde. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese nach dem Zufallsprinzip durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Dieses Ergebnis kann auf einen unbefugten Zugriff auf Ihre AWS Ressourcen hinweisen, mit der Absicht, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten S3-Buckets.

Suchtypen für EKS-Schutz

Die folgenden Ergebnisse beziehen sich spezifisch auf Amazon EKS-Ressourcen und haben einen resource_type von. `EKSCluster` Der Schweregrad und die Details der Erkenntnisse unterscheiden sich je nach Erkenntnistyp.

Für alle Ergebnisse vom Typ EKS-Audit-Logs empfehlen wir, dass Sie die betreffende Ressource untersuchen, um festzustellen, ob es sich bei der Aktivität um erwartete oder potenziell bösartige Aktivitäten handelt. Hinweise zur Behebung einer gefährdeten EKS-Auditprotokollressource, die durch einen GuardDuty Befund identifiziert wurde, finden Sie unter. Behebung der EKS-Schutzfeststellungen

> **Note**
>
> Wenn die Aktivität, aufgrund derer diese Erkenntnisse generiert werden, erwartet wird, sollten Sie erwägen, Unterdrückungsregeln in GuardDuty sie hinzuzufügen, um zukünftige Benachrichtigungen zu verhindern.

Themen

- CredentialAccess:Kubernetes/MaliciousIPCaller
- CredentialAccess:Kubernetes/MaliciousIPCaller.Custom
- CredentialAccess:Kubernetes/SuccessfulAnonymousAccess

- CredentialAccess:Kubernetes/TorIPCaller
- DefenseEvasion:Kubernetes/MaliciousIPCaller
- DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom
- DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess
- DefenseEvasion:Kubernetes/TorIPCaller
- Discovery:Kubernetes/MaliciousIPCaller
- Discovery:Kubernetes/MaliciousIPCaller.Custom
- Discovery:Kubernetes/SuccessfulAnonymousAccess
- Discovery:Kubernetes/TorIPCaller
- Execution:Kubernetes/ExecInKubeSystemPod
- Impact:Kubernetes/MaliciousIPCaller
- Impact:Kubernetes/MaliciousIPCaller.Custom
- Impact:Kubernetes/SuccessfulAnonymousAccess
- Impact:Kubernetes/TorIPCaller
- Persistence:Kubernetes/MaliciousIPCaller
- Persistence:Kubernetes/MaliciousIPCaller.Custom
- Persistence:Kubernetes/SuccessfulAnonymousAccess
- Persistence:Kubernetes/TorIPCaller
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount
- Policy:Kubernetes/AnonymousAccessGranted
- Policy:Kubernetes/ExposedDashboard
- Policy:Kubernetes/KubeflowDashboardExposed
- CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated
- Execution:Kubernetes/AnomalousBehavior.ExecInPod
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer
- Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount
- Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated
- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

> **Note**
>
> Vor Kubernetes Version 1.14 war die `system:unauthenticated` Gruppe standardmäßig mit und verknüpft. `system:discovery` `system:basic-user` ClusterRoles Diese Zuordnung kann unbeabsichtigten Zugriff durch anonyme Benutzer ermöglichen. Durch Cluster-Updates werden diese Berechtigungen nicht aufgehoben. Auch wenn Sie Ihren Cluster auf Version 1.14 oder höher aktualisiert haben, sind diese Berechtigungen möglicherweise weiterhin aktiviert. Wir empfehlen, dass Sie die Zuordnung dieser Berechtigungen zu der `system:unauthenticated`-Gruppe aufheben. Anleitungen zum Widerrufen dieser Berechtigungen finden Sie unter Bewährte Sicherheitsmethoden für Amazon EKS im Amazon EKS-Benutzerhandbuch.

CredentialAccess:Kubernetes/MaliciousIPCaller

Eine API, die häufig für den Zugriff auf Anmeldeinformationen oder Geheimnisse in einem Kubernetes-Cluster verwendet wird, wurde von einer bekannten bösartigen IP-Adresse aus aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang von einer IP-Adresse aus aufgerufen wurde, die mit bekannten böswilligen Aktivitäten in Verbindung steht. Die beobachtete API wird häufig mit der Phase des Zugriffs auf Anmeldeinformationen in Verbindung gebracht, wenn ein Angreifer versucht, Passwörter, Benutzernamen und Zugriffsschlüssel für Ihren Kubernetes-Cluster zu sammeln.

Empfehlungen zur Abhilfe:

Wenn der in der Erkenntnis unter dem Abschnitt `KubernetesUserDetails` angegebene Benutzer `system:anonymous` ist, untersuchen Sie, warum der anonyme Benutzer die API aufrufen durfte. Widerrufen Sie die Berechtigungen, falls erforderlich, indem Sie die Anweisungen unter Bewährte Methoden für die Sicherheit in Amazon EKS im Amazon-EKS-Benutzerhandbuch befolgen. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem

Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

CredentialAccess:Kubernetes/MaliciousIPCaller.Custom

Eine API, die häufig für den Zugriff auf Anmeldeinformationen oder Geheimnisse in einem Kubernetes-Cluster verwendet wird, wurde von einer IP-Adresse auf einer benutzerdefinierten Bedrohungsliste aus aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang von einer IP-Adresse aus aufgerufen wurde, die in einer von Ihnen hochgeladenen Bedrohungsliste enthalten ist. Die mit dieser Erkenntnis verknüpfte Bedrohungsliste ist im Abschnitt Zusätzliche Informationen der Details zu einer Erkenntnis aufgeführt. Die beobachtete API wird häufig mit der Taktik des Zugriffs auf Anmeldeinformationen in Verbindung gebracht, wenn ein Angreifer versucht, Passwörter, Benutzernamen und Zugriffsschlüssel für Ihren Kubernetes-Cluster zu sammeln.

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die API aufrufen durfte, und widerrufen Sie gegebenenfalls die Berechtigungen, indem Sie die Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im Amazon EKS-Benutzerhandbuch befolgen. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

CredentialAccess:Kubernetes/SuccessfulAnonymousAccess

Eine API, die häufig für den Zugriff auf Anmeldeinformationen oder Geheimnisse in einem Kubernetes-Cluster verwendet wird, wurde von einem nicht authentifizierten Benutzer aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang vom `system:anonymous`-Benutzer erfolgreich aufgerufen wurde. API-Aufrufe von `system:anonymous` sind nicht authentifiziert. Die beobachtete API wird häufig mit der Taktik des Zugriffs auf Anmeldeinformationen in Verbindung gebracht, wenn ein Angreifer versucht, Passwörter, Benutzernamen und Zugriffsschlüssel für Ihren Kubernetes-Cluster zu sammeln. Diese Aktivität weist darauf hin, dass anonymer oder nicht authentifizierter Zugriff auf die in der Erkenntnis gemeldete API-Aktion zulässig ist und bei anderen Aktionen möglicherweise zulässig ist. Wenn dieses Verhalten nicht erwartet wird, deutet dies möglicherweise auf einen Konfigurationsfehler hin oder darauf, dass Ihre Anmeldeinformationen kompromittiert wurden.

Empfehlungen zur Abhilfe:

Sie sollten die Berechtigungen überprüfen, die dem `system:anonymous`-Benutzer in Ihrem Cluster gewährt wurden, und sicherstellen, dass alle Berechtigungen benötigt werden. Wenn die Berechtigungen irrtümlich oder böswillig erteilt wurden, sollten Sie dem Benutzer den Zugriff entziehen und alle von einem Angreifer an Ihrem Cluster vorgenommenen Änderungen rückgängig machen. Weitere Informationen finden Sie unter Bewährte Methoden für die Sicherheit in Amazon EKS im Amazon-EKS-Benutzerhandbuch.

Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

CredentialAccess:Kubernetes/TorIPCaller

Eine API, die häufig für den Zugriff auf Anmeldeinformationen oder Geheimnisse in einem Kubernetes-Cluster verwendet wird, wurde von einer bekannten bösartigen Tor-Ausgangsknotens-Adresse aus aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Die Erkenntnis informiert Sie darüber, dass ein API-Vorgang von einer Tor-Ausgangsknotens-IP-Adresse aufgerufen wurde. Die beobachtete API wird häufig mit der Taktik des Zugriffs auf Anmeldeinformationen in Verbindung gebracht, wenn ein Angreifer versucht, Passwörter, Benutzernamen und Zugriffsschlüssel für Ihren Kubernetes-Cluster zu sammeln. Tor ist eine

Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese nach dem Zufallsprinzip durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Dies kann auf einen unbefugten Zugriff auf die Kubernetes-Cluster-Ressourcen hinweisen, mit dem Ziel, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Wenn der in der Erkenntnis unter dem Abschnitt `KubernetesUserDetails` angegebene Benutzer `system:anonymous` ist, untersuchen Sie, warum der anonyme Benutzer die API aufrufen durfte. Widerrufen Sie die Berechtigungen, falls erforderlich, indem Sie die Anweisungen unter Bewährte Methoden für die Sicherheit in Amazon EKS im Amazon-EKS-Benutzerhandbuch befolgen. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

DefenseEvasion:Kubernetes/MaliciousIPCaller

Eine API, die häufig verwendet wird, um Abwehrmaßnahmen zu umgehen, wurde von einer bekannten bösartigen IP-Adresse aus aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang von einer IP-Adresse aus aufgerufen wurde, die mit bekannten böswilligen Aktivitäten in Verbindung steht. Die beobachtete API wird häufig mit Umgehungstaktiken in Verbindung gebracht, bei denen ein Gegner versucht, seine Aktionen zu verbergen, um nicht entdeckt zu werden.

Empfehlungen zur Abhilfe:

Wenn der in der Erkenntnis unter dem Abschnitt `KubernetesUserDetails` angegebene Benutzer `system:anonymous` ist, untersuchen Sie, warum der anonyme Benutzer die API aufrufen durfte. Widerrufen Sie die Berechtigungen, falls erforderlich, indem Sie die Anweisungen unter Bewährte Methoden für die Sicherheit in Amazon EKS im Amazon-EKS-Benutzerhandbuch befolgen. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität

legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom

Eine API, die üblicherweise zur Umgehung von Abwehrmaßnahmen verwendet wird, wurde von einer IP-Adresse auf einer benutzerdefinierten Bedrohungsliste aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang von einer IP-Adresse aus aufgerufen wurde, die in einer von Ihnen hochgeladenen Bedrohungsliste enthalten ist. Die mit dieser Erkenntnis verknüpfte Bedrohungsliste ist im Abschnitt Zusätzliche Informationen der Details zu einer Erkenntnis aufgeführt. Die beobachtete API wird häufig mit Umgehungstaktiken in Verbindung gebracht, bei denen ein Gegner versucht, seine Aktionen zu verbergen, um nicht entdeckt zu werden.

Empfehlungen zur Abhilfe:

Wenn der in der Erkenntnis unter dem Abschnitt `KubernetesUserDetails` angegebene Benutzer `system:anonymous` ist, untersuchen Sie, warum der anonyme Benutzer die API aufrufen durfte. Widerrufen Sie die Berechtigungen, falls erforderlich, indem Sie die Anweisungen unter Bewährte Methoden für die Sicherheit in Amazon EKS im Amazon-EKS-Benutzerhandbuch befolgen. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess

Eine API, die häufig verwendet wird, um Abwehrmaßnahmen zu umgehen, wurde von einem nicht authentifizierten Benutzer aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang vom `system:anonymous`-Benutzer erfolgreich aufgerufen wurde. API-Aufrufe von `system:anonymous` sind nicht authentifiziert. Die beobachtete API wird häufig mit Taktiken zur Umgehung der Verteidigung in Verbindung gebracht, bei der ein Gegner versucht, seine Aktionen zu verbergen, um nicht entdeckt zu werden. Diese Aktivität weist darauf hin, dass anonymer oder nicht authentifizierter Zugriff auf die in der Erkenntnis gemeldete API-Aktion zulässig ist und bei anderen Aktionen möglicherweise zulässig ist. Wenn dieses Verhalten nicht erwartet wird, deutet dies möglicherweise auf einen Konfigurationsfehler hin oder darauf, dass Ihre Anmeldeinformationen kompromittiert wurden.

Empfehlungen zur Abhilfe:

Sie sollten die Berechtigungen überprüfen, die dem `system:anonymous`-Benutzer in Ihrem Cluster gewährt wurden, und sicherstellen, dass alle Berechtigungen benötigt werden. Wenn die Berechtigungen irrtümlich oder böswillig erteilt wurden, sollten Sie dem Benutzer den Zugriff entziehen und alle von einem Angreifer an Ihrem Cluster vorgenommenen Änderungen rückgängig machen. Weitere Informationen finden Sie unter Bewährte Methoden für die Sicherheit in Amazon EKS im Amazon-EKS-Benutzerhandbuch.

Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

DefenseEvasion:Kubernetes/TorIPCaller

Eine API, die häufig verwendet wird, um Abwehrmaßnahmen zu umgehen, wurde von einer IP-Adresse des Tor-Ausgangsknotens aus aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Die Erkenntnis informiert Sie darüber, dass ein API-Vorgang von einer Tor-Ausgangsknotens-IP-Adresse aufgerufen wurde. Die beobachtete API wird häufig mit Umgehungstaktiken in Verbindung gebracht, bei denen ein Gegner versucht, seine Aktionen zu verbergen, um nicht entdeckt zu werden. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese nach dem Zufallsprinzip durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird Exit-Knoten genannt. Dies kann auf einen unbefugten Zugriff auf Ihren Kubernetes-Cluster hinweisen, der das Ziel hat, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Wenn der in der Erkenntnis unter dem Abschnitt `KubernetesUserDetails` angegebene Benutzer `system:anonymous` ist, untersuchen Sie, warum der anonyme Benutzer die API aufrufen durfte. Widerrufen Sie die Berechtigungen, falls erforderlich, indem Sie die Anweisungen unter Bewährte Methoden für die Sicherheit in Amazon EKS im Amazon-EKS-Benutzerhandbuch befolgen. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

Discovery:Kubernetes/MaliciousIPCaller

Eine API, die häufig zur Erkennung von Ressourcen in einem Kubernetes-Cluster verwendet wird, wurde von einer IP-Adresse aus aufgerufen.

Standard-Schweregrad: Mittel

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang von einer IP-Adresse aus aufgerufen wurde, die mit bekannten böswilligen Aktivitäten in Verbindung steht. Die beobachtete API wird häufig in der Erkennungsphase eines Angriffs verwendet, in der ein Angreifer Informationen sammelt, um festzustellen, ob Ihr Kubernetes-Cluster für einen umfassenderen Angriff anfällig ist.

> Für nicht authentifizierten Zugriff
>
> MaliciousIPCallerFür einen nicht authentifizierten Zugriff werden keine Ergebnisse generiert. SuccessfulAnonymousAccessErgebnisse werden für einen nicht authentifizierten oder anonymen Zugriff generiert.

Empfehlungen zur Abhilfe:

Wenn der in der Erkenntnis unter dem Abschnitt `KubernetesUserDetails` angegebene Benutzer `system:anonymous` ist, untersuchen Sie, warum der anonyme Benutzer die API aufrufen durfte. Widerrufen Sie die Berechtigungen, falls erforderlich, indem Sie die Anweisungen unter Bewährte

Methoden für die Sicherheit in Amazon EKS im Amazon-EKS-Benutzerhandbuch befolgen. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

Discovery:Kubernetes/MaliciousIPCaller.Custom

Eine API, die häufig zur Erkennung von Ressourcen in einem Kubernetes-Cluster verwendet wird, wurde von einer IP-Adresse aus einer benutzerdefinierten Bedrohungsliste aufgerufen.

Standard-Schweregrad: Mittel

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass eine API von einer IP-Adresse aufgerufen wurde, die in einer von Ihnen hochgeladenen Bedrohungsliste enthalten ist. Die mit dieser Erkenntnis verknüpfte Bedrohungsliste ist im Abschnitt Zusätzliche Informationen der Details zu einer Erkenntnis aufgeführt. Die beobachtete API wird häufig in der Erkennungsphase eines Angriffs verwendet, in der ein Angreifer Informationen sammelt, um festzustellen, ob Ihr Kubernetes-Cluster für einen umfassenderen Angriff anfällig ist.

Empfehlungen zur Abhilfe:

Wenn der in der Erkenntnis unter dem Abschnitt `KubernetesUserDetails` angegebene Benutzer `system:anonymous` ist, untersuchen Sie, warum der anonyme Benutzer die API aufrufen durfte. Widerrufen Sie die Berechtigungen, falls erforderlich, indem Sie die Anweisungen unter Bewährte Methoden für die Sicherheit in Amazon EKS im Amazon-EKS-Benutzerhandbuch befolgen. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

Discovery:Kubernetes/SuccessfulAnonymousAccess

Eine API, die häufig zur Erkennung von Ressourcen in einem Kubernetes-Cluster verwendet wird, wurde von einem nicht authentifizierten Benutzer aufgerufen.

Standard-Schweregrad: Mittel

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang vom `system:anonymous`-Benutzer erfolgreich aufgerufen wurde. API-Aufrufe von `system:anonymous` sind nicht authentifiziert. Die beobachtete API wird häufig mit der Erkennungsphase eines Angriffs in Verbindung gebracht, in der ein Angreifer Informationen über Ihren Kubernetes-Cluster sammelt. Diese Aktivität weist darauf hin, dass anonymer oder nicht authentifizierter Zugriff auf die in der Erkenntnis gemeldete API-Aktion zulässig ist und bei anderen Aktionen möglicherweise zulässig ist. Wenn dieses Verhalten nicht erwartet wird, deutet dies möglicherweise auf einen Konfigurationsfehler hin oder darauf, dass Ihre Anmeldeinformationen kompromittiert wurden.

Dieser Ergebnistyp schließt API-Endpunkte wie`/healthz`, `/livez/readyz`, und aus. `/version`

Empfehlungen zur Abhilfe:

Sie sollten die Berechtigungen überprüfen, die dem `system:anonymous`-Benutzer in Ihrem Cluster gewährt wurden, und sicherstellen, dass alle Berechtigungen benötigt werden. Wenn die Berechtigungen irrtümlich oder böswillig erteilt wurden, sollten Sie dem Benutzer den Zugriff entziehen und alle von einem Angreifer an Ihrem Cluster vorgenommenen Änderungen rückgängig machen. Weitere Informationen finden Sie unter Bewährte Methoden für die Sicherheit in Amazon EKS im Amazon-EKS-Benutzerhandbuch.

Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

Discovery:Kubernetes/TorIPCaller

Eine API, die häufig zur Erkennung von Ressourcen in einem Kubernetes-Cluster verwendet wird, wurde von einer IP-Adresse des Tor-Ausgangsknotens aus aufgerufen.

Standard-Schweregrad: Mittel

- Funktion: EKS-Auditprotokolle

Die Erkenntnis informiert Sie darüber, dass ein API-Vorgang von einer Tor-Ausgangsknotens-IP-Adresse aufgerufen wurde. Die beobachtete API wird häufig in der Erkennungsphase eines Angriffs verwendet, in der ein Angreifer Informationen sammelt, um festzustellen, ob Ihr Kubernetes-Cluster für einen umfassenderen Angriff anfällig ist. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese nach dem Zufallsprinzip durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird Exit-Knoten genannt. Dies kann auf einen unbefugten Zugriff auf Ihren Kubernetes-Cluster hinweisen, der das Ziel hat, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die API aufrufen durfte, und widerrufen Sie gegebenenfalls die Berechtigungen, indem Sie die Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im Amazon EKS-Benutzerhandbuch befolgen. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

Execution:Kubernetes/ExecInKubeSystemPod

`Ein Befehl wurde in einem Pod im Kube-System-Namespace ausgeführt`

Standard-Schweregrad: Mittel

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein Befehl in einem Pod innerhalb des `kube-system`-Namespace mithilfe der Kubernetes-Exec-API ausgeführt wurde. `kube-system`-Namespace ist ein Standard-Namespaces, der hauptsächlich für Komponenten auf Systemebene wie `kube-dns` und `kube-proxy` verwendet wird. Es ist sehr ungewöhnlich, Befehle innerhalb von Pods oder Containern unter einem `kube-system`-Namespace auszuführen, was auf verdächtige Aktivitäten hinweisen kann.

Empfehlungen zur Abhilfe:

Wenn die Ausführung dieses Befehls unerwartet erfolgt, können die Anmeldeinformationen der Benutzeridentität, die zur Ausführung des Befehls verwendet wurde, kompromittiert sein. Sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

Impact:Kubernetes/MaliciousIPCaller

Eine API, die häufig zur Manipulation von Ressourcen in einem Kubernetes-Cluster verwendet wird, wurde von einer bekannten bösartigen IP-Adresse aus aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang von einer IP-Adresse aus aufgerufen wurde, die mit bekannten böswilligen Aktivitäten in Verbindung steht. Die beobachtete API wird häufig mit Schlagtaktiken in Verbindung gebracht, bei denen ein Angreifer versucht, Daten in Ihrer Umgebung zu manipulieren, zu unterbrechen oder zu zerstören. AWS

Empfehlungen zur Abhilfe:

Wenn der in der Erkenntnis unter dem Abschnitt `KubernetesUserDetails` angegebene Benutzer `system:anonymous` ist, untersuchen Sie, warum der anonyme Benutzer die API aufrufen durfte. Widerrufen Sie die Berechtigungen, falls erforderlich, indem Sie die Anweisungen unter Bewährte Methoden für die Sicherheit in Amazon EKS im Amazon-EKS-Benutzerhandbuch befolgen. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

Impact:Kubernetes/MaliciousIPCaller.Custom

Eine API, die häufig zur Manipulation von Ressourcen in einem Kubernetes-Cluster verwendet wird, wurde von einer IP-Adresse auf einer benutzerdefinierten Bedrohungsliste aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang von einer IP-Adresse aus aufgerufen wurde, die in einer von Ihnen hochgeladenen Bedrohungsliste enthalten ist. Die mit dieser Erkenntnis verknüpfte Bedrohungsliste ist im Abschnitt Zusätzliche Informationen der Details zu einer Erkenntnis aufgeführt. Die beobachtete API wird häufig mit Schlagtaktiken in Verbindung gebracht, bei denen ein Angreifer versucht, Daten in Ihrer Umgebung zu manipulieren, zu unterbrechen oder zu zerstören. AWS

Empfehlungen zur Abhilfe:

Wenn der in der Erkenntnis unter dem Abschnitt `KubernetesUserDetails` angegebene Benutzer `system:anonymous` ist, untersuchen Sie, warum der anonyme Benutzer die API aufrufen durfte. Widerrufen Sie die Berechtigungen, falls erforderlich, indem Sie die Anweisungen unter Bewährte Methoden für die Sicherheit in Amazon EKS im Amazon-EKS-Benutzerhandbuch befolgen. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

Impact:Kubernetes/SuccessfulAnonymousAccess

Eine API, die häufig zur Manipulation von Ressourcen in einem Kubernetes-Cluster verwendet wird, wurde von einem nicht authentifizierten Benutzer aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang vom `system:anonymous`-Benutzer erfolgreich aufgerufen wurde. API-Aufrufe von `system:anonymous` sind nicht authentifiziert. Die beobachtete API wird häufig mit der Auswirkungsphase eines Angriffs in Verbindung gebracht, wenn ein Angreifer Ressourcen in Ihrem Cluster manipuliert. Diese Aktivität weist darauf hin, dass anonymer oder nicht authentifizierter Zugriff auf die in der Erkenntnis gemeldete API-Aktion zulässig ist und bei anderen Aktionen möglicherweise zulässig ist. Wenn dieses Verhalten nicht erwartet wird, deutet dies möglicherweise auf einen Konfigurationsfehler hin oder darauf, dass Ihre Anmeldeinformationen kompromittiert wurden.

Empfehlungen zur Abhilfe:

Sie sollten die Berechtigungen überprüfen, die dem `system:anonymous`-Benutzer in Ihrem Cluster gewährt wurden, und sicherstellen, dass alle Berechtigungen benötigt werden. Wenn die Berechtigungen irrtümlich oder böswillig erteilt wurden, sollten Sie dem Benutzer den Zugriff entziehen und alle von einem Angreifer an Ihrem Cluster vorgenommenen Änderungen rückgängig machen. Weitere Informationen finden Sie unter Bewährte Methoden für die Sicherheit in Amazon EKS im Amazon-EKS-Benutzerhandbuch.

Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

Impact:Kubernetes/TorIPCaller

Eine API, die häufig verwendet wird, um Ressourcen in einem Kubernetes-Cluster zu manipulieren, wurde von einer IP-Adresse des Tor-Ausgangsknotens aus aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Die Erkenntnis informiert Sie darüber, dass ein API-Vorgang von einer Tor-Ausgangsknotens-IP-Adresse aufgerufen wurde. Die beobachtete API wird häufig mit Auswirkungstaktiken in Verbindung gebracht, bei denen ein Angreifer versucht, Daten in Ihrer AWS -Umgebung zu manipulieren, zu unterbrechen oder zu zerstören. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese nach dem Zufallsprinzip durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird Exit-Knoten genannt. Dies kann auf einen unbefugten Zugriff auf Ihren Kubernetes-Cluster hinweisen, der das Ziel hat, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Wenn der in der Erkenntnis unter dem Abschnitt `KubernetesUserDetails` angegebene Benutzer `system:anonymous` ist, untersuchen Sie, warum der anonyme Benutzer die API aufrufen durfte. Widerrufen Sie die Berechtigungen, falls erforderlich, indem Sie die Anweisungen unter Bewährte Methoden für die Sicherheit in Amazon EKS im Amazon-EKS-Benutzerhandbuch befolgen. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

Persistence:Kubernetes/MaliciousIPCaller

Eine API, die üblicherweise verwendet wird, um dauerhaften Zugriff auf einen Kubernetes-Cluster zu erhalten, wurde von einer bekannten bösartigen IP-Adresse aus aufgerufen.

Standard-Schweregrad: Mittel

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang von einer IP-Adresse aus aufgerufen wurde, die mit bekannten böswilligen Aktivitäten in Verbindung steht. Die beobachtete API wird häufig mit Persistenz-Taktiken in Verbindung gebracht, bei denen sich ein Angreifer Zugriff auf Ihren Kubernetes-Cluster verschafft hat und versucht, diesen Zugriff aufrechtzuerhalten.

Empfehlungen zur Abhilfe:

Wenn der in der Erkenntnis unter dem Abschnitt `KubernetesUserDetails` angegebene Benutzer `system:anonymous` ist, untersuchen Sie, warum der anonyme Benutzer die API aufrufen durfte. Widerrufen Sie die Berechtigungen, falls erforderlich, indem Sie die Anweisungen unter Bewährte Methoden für die Sicherheit in Amazon EKS im Amazon-EKS-Benutzerhandbuch befolgen. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

Persistence:Kubernetes/MaliciousIPCaller.Custom

Eine API, die häufig verwendet wird, um dauerhaften Zugriff auf einen Kubernetes-Cluster zu erhalten, wurde von einer IP-Adresse aus einer benutzerdefinierten Bedrohungsliste aufgerufen.

Standard-Schweregrad: Mittel

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang von einer IP-Adresse aus aufgerufen wurde, die in einer von Ihnen hochgeladenen Bedrohungsliste enthalten ist. Die mit dieser Erkenntnis verknüpfte Bedrohungsliste ist im Abschnitt Zusätzliche Informationen der Details zu einer Erkenntnis aufgeführt. Die beobachtete API wird häufig mit Persistenz-Taktiken in Verbindung gebracht, bei denen sich ein Angreifer Zugriff auf Ihren Kubernetes-Cluster verschafft hat und versucht, diesen Zugriff aufrechtzuerhalten.

Empfehlungen zur Abhilfe:

Wenn der in der Erkenntnis unter dem Abschnitt `KubernetesUserDetails` angegebene Benutzer `system:anonymous` ist, untersuchen Sie, warum der anonyme Benutzer die API aufrufen durfte. Widerrufen Sie die Berechtigungen, falls erforderlich, indem Sie die Anweisungen unter Bewährte Methoden für die Sicherheit in Amazon EKS im Amazon-EKS-Benutzerhandbuch befolgen. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

Persistence:Kubernetes/SuccessfulAnonymousAccess

Eine API, die häufig verwendet wird, um hochgradige Berechtigungen für einen Kubernetes-Cluster zu erhalten, wurde von einem nicht authentifizierten Benutzer aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang vom `system:anonymous`-Benutzer erfolgreich aufgerufen wurde. API-Aufrufe von `system:anonymous` sind nicht authentifiziert. Die beobachtete API wird häufig mit Persistenztaktiken in Verbindung gebracht, bei denen sich ein Angreifer Zugriff auf Ihren Cluster verschafft hat und versucht, diesen Zugriff aufrechtzuerhalten. Diese Aktivität weist darauf hin, dass anonymer oder nicht authentifizierter Zugriff auf die in der Erkenntnis gemeldete API-Aktion zulässig ist und bei anderen Aktionen möglicherweise zulässig ist. Wenn dieses Verhalten nicht erwartet wird, deutet dies möglicherweise auf einen Konfigurationsfehler hin oder darauf, dass Ihre Anmeldeinformationen kompromittiert wurden.

Empfehlungen zur Abhilfe:

Sie sollten die Berechtigungen überprüfen, die dem `system:anonymous`-Benutzer in Ihrem Cluster gewährt wurden, und sicherstellen, dass alle Berechtigungen benötigt werden. Wenn die Berechtigungen irrtümlich oder böswillig erteilt wurden, sollten Sie dem Benutzer den Zugriff entziehen und alle von einem Angreifer an Ihrem Cluster vorgenommenen Änderungen rückgängig machen. Weitere Informationen finden Sie unter Bewährte Methoden für die Sicherheit in Amazon EKS im Amazon-EKS-Benutzerhandbuch.

Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

Persistence:Kubernetes/TorIPCaller

Eine API, die häufig verwendet wird, um dauerhaften Zugriff auf einen Kubernetes-Cluster zu erhalten, wurde von einer IP-Adresse des Tor-Ausgangsknotens aus aufgerufen.

Standard-Schweregrad: Mittel

- Funktion: EKS-Auditprotokolle

Die Erkenntnis informiert Sie darüber, dass ein API-Vorgang von einer Tor-Ausgangsknotens-IP-Adresse aufgerufen wurde. Die beobachtete API wird häufig mit Persistenz-Taktiken in Verbindung gebracht, bei denen sich ein Angreifer Zugriff auf Ihren Kubernetes-Cluster verschafft hat und versucht, diesen Zugriff aufrechtzuerhalten. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese nach dem Zufallsprinzip durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Dies kann auf einen unbefugten Zugriff auf Ihre AWS Ressourcen hinweisen, mit der Absicht, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Wenn der in der Erkenntnis unter dem Abschnitt `KubernetesUserDetails` angegebene Benutzer `system:anonymous` ist, untersuchen Sie, warum der anonyme Benutzer die API aufrufen durfte. Widerrufen Sie die Berechtigungen, falls erforderlich, indem Sie die Anweisungen unter Bewährte Methoden für die Sicherheit in Amazon EKS im Amazon-EKS-Benutzerhandbuch befolgen. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

Policy:Kubernetes/AdminAccessToDefaultServiceAccount

Dem Standard-Servicekonto wurden Administratorrechte auf einem Kubernetes-Cluster gewährt.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass dem Standard-Servicekonto für einen Namespace in Ihrem Kubernetes-Cluster Administratorrechte gewährt wurden. Kubernetes erstellt ein Standard-Servicekonto für alle Namespaces im Cluster. Es weist Pods, die nicht explizit einem anderen Servicekonto zugeordnet wurden, automatisch das Standard-Servicekonto als Identität zu. Wenn das Standard-Servicekonto über Administratorrechte verfügt, kann dies dazu führen, dass Pods unbeabsichtigt mit Administratorrechten gestartet werden. Wenn dieses Verhalten nicht erwartet wird, deutet dies möglicherweise auf einen Konfigurationsfehler hin oder darauf, dass Ihre Anmeldeinformationen kompromittiert wurden.

Empfehlungen zur Abhilfe:

Sie sollten nicht das Standard-Servicekonto verwenden, um Pods Berechtigungen zu erteilen. Stattdessen sollten Sie für jeden Workload ein eigenes Servicekonto erstellen und diesem Konto je nach Bedarf Berechtigungen erteilen. Um dieses Problem zu beheben, sollten Sie spezielle Servicekonten für all Ihre Pods und Workloads erstellen und die Pods und Workloads aktualisieren, um vom Standard-Servicekonto zu ihren dedizierten Konten zu migrieren. Anschließend sollten Sie die Administratorberechtigung aus dem Standard-Servicekonto entfernen. Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

Policy:Kubernetes/AnonymousAccessGranted

Dem Benutzer **`system:anonymous`** wurde die API-Berechtigung für einen Kubernetes-Cluster erteilt.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein Benutzer in Ihrem Kubernetes-Cluster erfolgreich ein `ClusterRoleBinding` oder `RoleBinding` erstellt hat, um den Benutzer `system:anonymous` an eine Rolle zu binden. Dies ermöglicht einen nicht authentifizierten Zugriff auf die API-Vorgänge, die von der Rolle zugelassen werden. Wenn dieses Verhalten nicht erwartet wird, deutet dies möglicherweise auf einen Konfigurationsfehler hin oder darauf, dass Ihre Anmeldeinformationen kompromittiert wurden.

Empfehlungen zur Abhilfe:

Sie sollten die Berechtigungen überprüfen, die dem `system:anonymous`-Benutzer oder der `system:unauthenticated`-Gruppe in Ihrem Cluster gewährt wurden, und unnötigen anonymen Zugriff widerrufen. Weitere Informationen finden Sie unter Bewährte Methoden für die Sicherheit in Amazon EKS im Amazon-EKS-Benutzerhandbuch. Wenn die Berechtigungen irrtümlich oder böswillig erteilt wurden, sollten Sie dem Benutzer den Zugriff entziehen und alle von einem Angreifer an Ihrem Cluster vorgenommenen Änderungen rückgängig machen. Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

Policy:Kubernetes/ExposedDashboard

Das Dashboard für einen Kubernetes-Cluster war im Internet verfügbar

Standard-Schweregrad: Mittel

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass das Kubernetes-Dashboard für Ihren Cluster über einen Load Balancer-Service dem Internet zugänglich gemacht wurde. Ein offengelegtes Dashboard ermöglicht den Zugriff auf die Verwaltungsoberfläche Ihres Clusters über das Internet und ermöglicht es Gegnern, eventuell vorhandene Lücken in der Authentifizierungs- und Zugriffssteuerung auszunutzen.

Empfehlungen zur Abhilfe:

Sie sollten sicherstellen, dass im Kubernetes-Dashboard eine starke Authentifizierung und Autorisierung durchgesetzt wird. Sie sollten auch eine Netzwerk-Zugriffssteuerung implementieren, um den Zugriff auf das Dashboard von bestimmten IP-Adressen aus zu beschränken.

Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

Policy:Kubernetes/KubeflowDashboardExposed

Das Tool Kubeflow Das Dashboard für einen Kubernetes-Cluster war dem Internet zugänglich

Standard-Schweregrad: Mittel

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass das Kubeflow-Dashboard für Ihren Cluster über einen Load Balancer-Service dem Internet zugänglich gemacht wurde. Ein offengelegtes Kubeflow-Dashboard ermöglicht den Zugriff auf die Verwaltungsoberfläche Ihrer Kubeflow-Umgebung über das Internet und ermöglicht es Gegnern, eventuell vorhandene Lücken in der Authentifizierung und Zugriffssteuerung auszunutzen.

Empfehlungen zur Abhilfe:

Sie sollten sicherstellen, dass im Kubeflow-Dashboard eine starke Authentifizierung und Autorisierung durchgesetzt wird. Sie sollten auch eine Netzwerk-Zugriffssteuerung implementieren, um den Zugriff auf das Dashboard von bestimmten IP-Adressen aus zu beschränken.

Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed

Eine Kubernetes-API, die häufig für den Zugriff auf Geheimnisse verwendet wird, wurde auf ungewöhnliche Weise aufgerufen.

Standard-Schweregrad: Mittel

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein Kubernetes-Benutzer in Ihrem Cluster einen anomalen API-Vorgang zum Abrufen vertraulicher Cluster-Geheimnisse aufgerufen hat. Die beobachtete API wird häufig mit Taktiken für den Zugriff auf Anmeldeinformationen in Verbindung gebracht, die zu einer privilegierten Eskalation und weiterem Zugriff innerhalb Ihres Clusters führen können. Wenn dieses Verhalten nicht erwartet wird, deutet dies möglicherweise auf einen Konfigurationsfehler hin oder darauf, dass Ihre AWS -Anmeldeinformationen kompromittiert wurden.

Die beobachtete API wurde anhand des ML-Modells (Machine Learning) zur Erkennung von GuardDuty Anomalien als anomal identifiziert. Das ML-Modell bewertet alle Benutzer-API-Aktivitäten innerhalb Ihres EKS-Clusters und identifiziert anomale Ereignisse, die mit Techniken in Verbindung stehen, die von nicht autorisierten Benutzern verwendet werden. Das ML-Modell verfolgt mehrere Faktoren des API-Vorgangs, z. B. den Benutzer, der die Anfrage stellt, den Standort, von dem aus die Anfrage gestellt wurde, den verwendeten Benutzeragenten und den Namespace, den der Benutzer verwendet hat. Die ungewöhnlichen Details der API-Anfrage finden Sie im Bereich mit den Suchdetails in der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Sie sollten die Berechtigungen überprüfen, die dem Kubernetes-Benutzer in Ihrem Cluster gewährt wurden, und sicherstellen, dass all diese Berechtigungen benötigt werden. Wenn die Berechtigungen irrtümlich oder böswillig erteilt wurden, sollten Sie dem Benutzer den Zugriff entziehen und alle von einem Angreifer an Ihrem Cluster vorgenommenen Änderungen rückgängig machen. Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

Falls Ihre AWS Anmeldeinformationen kompromittiert wurden, finden Sie weitere Informationen unterBehebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated

In Ihrem RoleBinding ClusterRoleBinding Kubernetes-Cluster wurde ein oder für eine übermäßig freizügige Rolle oder einen sensiblen Namespace erstellt oder geändert.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn ein RoleBinding oder jedoch das Oder ClusterRoleBinding beinhaltet, ist der Schweregrad Hoch ClusterRoles `admin`. `cluster-admin`

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein Benutzer in Ihrem Kubernetes-Cluster ein `RoleBinding` oder `ClusterRoleBinding` erstellt hat, um einen Benutzer an eine Rolle mit Administratorberechtigungen oder sensiblen Namespaces zu binden. Wenn dieses Verhalten nicht erwartet wird, deutet dies möglicherweise auf einen Konfigurationsfehler hin oder darauf, dass Ihre AWS -Anmeldeinformationen kompromittiert wurden.

Die beobachtete API wurde anhand des ML-Modells (Machine Learning) zur Erkennung von GuardDuty Anomalien als anomal identifiziert. Das ML-Modell bewertet alle Benutzer-API-Aktivitäten innerhalb Ihres EKS-Clusters. Dieses ML-Modell identifiziert auch ungewöhnliche Ereignisse, die mit den von einem nicht autorisierten Benutzer verwendeten Techniken zusammenhängen. Das ML-Modell verfolgt mehrere Faktoren des API-Vorgangs, z. B. den Benutzer, der die Anfrage stellt, den Standort, von dem aus die Anfrage gestellt wurde, den verwendeten Benutzeragenten und den Namespace, den der Benutzer verwendet hat. Die ungewöhnlichen Details der API-Anfrage finden Sie im Bereich mit den Suchdetails in der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Untersuchen Sie die dem Kubernetes-Benutzer erteilten Berechtigungen. Diese Berechtigungen sind in der Rolle und den beteiligten Subjekten in `RoleBinding` und `ClusterRoleBinding` definiert. Wenn die Berechtigungen irrtümlich oder böswillig erteilt wurden, sollten Sie dem Benutzer den Zugriff entziehen und alle von einem Angreifer an Ihrem Cluster vorgenommenen Änderungen rückgängig machen. Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

Falls Ihre AWS Anmeldeinformationen kompromittiert wurden, finden Sie weitere Informationen unterBehebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

Execution:Kubernetes/AnomalousBehavior.ExecInPod

Ein Befehl wurde in einem Pod auf ungewöhnliche Weise ausgeführt.

Standard-Schweregrad: Mittel

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein Befehl in einem Pod mithilfe der Kubernetes-Exec-API ausgeführt wurde. Die Kubernetes-Exec-API ermöglicht die Ausführung beliebiger Befehle in

einem Pod. Wenn dieses Verhalten für den Benutzer, den Namespace oder den Pod nicht erwartet wird, kann dies entweder auf einen Konfigurationsfehler hinweisen oder darauf, dass Ihre AWS Anmeldeinformationen kompromittiert wurden.

Die beobachtete API wurde durch das ML-Modell (Machine Learning) zur Erkennung von GuardDuty Anomalien als anomal identifiziert. Das ML-Modell bewertet alle Benutzer-API-Aktivitäten innerhalb Ihres EKS-Clusters. Dieses ML-Modell identifiziert auch ungewöhnliche Ereignisse, die mit den von einem nicht autorisierten Benutzer verwendeten Techniken zusammenhängen. Das ML-Modell verfolgt mehrere Faktoren des API-Vorgangs, z. B. den Benutzer, der die Anfrage stellt, den Standort, von dem aus die Anfrage gestellt wurde, den verwendeten Benutzeragenten und den Namespace, den der Benutzer verwendet hat. Die ungewöhnlichen Details der API-Anfrage finden Sie im Bereich mit den Suchdetails in der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Wenn die Ausführung dieses Befehls unerwartet erfolgt, wurden möglicherweise die Anmeldeinformationen der Benutzeridentität, die zur Ausführung des Befehls verwendet wurde, kompromittiert. Sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

Falls Ihre AWS Anmeldeinformationen kompromittiert wurden, finden Sie weitere Informationen unterBehebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer

Ein Workload wurde mit einem privilegierten Container auf ungewöhnliche Weise gestartet.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein Workload mit einem privilegierten Container in Ihrem Amazon-EKS-Cluster gestartet wurde. Ein privilegierter Container hat Zugriff auf Root-Ebene auf den Host. Unbefugte Benutzer können privilegierte Container als Taktik zur Rechteerweiterung starten, um sich zunächst Zugriff auf den Host zu verschaffen und ihn dann zu kompromittieren.

Die beobachtete Erstellung oder Änderung eines Containers wurde anhand des ML-Modells (Machine Learning) zur Erkennung von GuardDuty Anomalien als anomal identifiziert. Das ML-Modell bewertet alle Benutzer-API- und Container-Image-Aktivitäten innerhalb Ihres EKS-Clusters. Dieses ML-Modell identifiziert auch ungewöhnliche Ereignisse, die mit den von einem nicht autorisierten Benutzer verwendeten Techniken zusammenhängen. Das ML-Modell verfolgt mehrere Faktoren des API-Vorgangs, z. B. den Benutzer, der die Anfrage stellt, den Standort, von dem aus die Anfrage gestellt wurde, den verwendeten Benutzeragenten, in Ihrem Konto beobachtete Container-Images und den Namespace, den der Benutzer verwendet hat. Die ungewöhnlichen Details der API-Anfrage finden Sie im Bereich mit den Suchdetails in der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Wenn dieser Container-Start unerwartet erfolgt, wurden möglicherweise die Anmeldeinformationen der Benutzeridentität, die zum Starten des Containers verwendet wurde, kompromittiert. Sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

Falls Ihre AWS Anmeldeinformationen kompromittiert wurden, finden Sie weitere Informationen unterBehebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

Wenn dieser Container-Start erwartet wird, empfiehlt es sich, eine Unterdrückungsregel mit Filterkriterien zu verwenden, die auf dem `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`-Feld basieren. In den Filterkriterien sollte das `imagePrefix`-Feld dem in der Erkenntnis angegebenen Feld `imagePrefix` entsprechen. Weitere Informationen finden Sie unter Unterdrückungsregeln in GuardDuty.

Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount

Ein Workload wurde auf ungewöhnliche Weise bereitgestellt, wobei ein sensibler Host-Pfad innerhalb des Workloads eingehängt wurde.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein Workload mit einem Container gestartet wurde, der im Abschnitt `volumeMounts` einen sensiblen Host-Pfad enthielt. Dadurch ist der sensible Host-Pfad potenziell vom Container aus zugänglich und beschreibbar. Diese Technik wird häufig von Gegnern verwendet, um Zugriff auf das Dateisystem des Hosts zu erhalten.

Die beobachtete Erstellung oder Änderung eines Containers wurde anhand des ML-Modells (Machine Learning) zur Erkennung von GuardDuty Anomalien als anomal identifiziert. Das ML-Modell bewertet alle Benutzer-API- und Container-Image-Aktivitäten innerhalb Ihres EKS-Clusters. Dieses ML-Modell identifiziert auch ungewöhnliche Ereignisse, die mit den von einem nicht autorisierten Benutzer verwendeten Techniken zusammenhängen. Das ML-Modell verfolgt mehrere Faktoren des API-Vorgangs, z. B. den Benutzer, der die Anfrage stellt, den Standort, von dem aus die Anfrage gestellt wurde, den verwendeten Benutzeragenten, in Ihrem Konto beobachtete Container-Images und den Namespace, den der Benutzer verwendet hat. Die ungewöhnlichen Details der API-Anfrage finden Sie im Bereich mit den Suchdetails in der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Wenn dieser Container-Start unerwartet erfolgt, wurden möglicherweise die Anmeldeinformationen der Benutzeridentität, die zum Starten des Containers verwendet wurde, kompromittiert. Sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

Falls Ihre AWS Anmeldeinformationen kompromittiert wurden, finden Sie weitere Informationen unterBehebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

Wenn dieser Container-Start erwartet wird, empfiehlt es sich, eine Unterdrückungsregel mit Filterkriterien zu verwenden, die auf dem `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`-Feld basieren. In den Filterkriterien sollte das `imagePrefix`-Feld dem in der Erkenntnis angegebenen Feld `imagePrefix` entsprechen. Weitere Informationen finden Sie unter Unterdrückungsregeln in GuardDuty.

Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed

Ein Workload wurde auf ungewöhnliche Weise gestartet.

Standard-Schweregrad: Niedrig*

> **Note**
>
> Der Standardschweregrad ist Niedrig. Wenn der Workload jedoch einen potenziell verdächtigen Image-Namen enthält, z. B. ein bekanntes Pentest-Tool, oder einen Container, in dem beim Start ein potenziell verdächtiger Befehl ausgeführt wird, z. B. Reverse-Shell-Befehle, wird der Schweregrad dieses Ergebnistyps als Mittel eingestuft.

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein Kubernetes-Workload in Ihrem Amazon EKS-Cluster auf ungewöhnliche Weise erstellt oder geändert wurde, z. B. durch eine API-Aktivität, neue Container-Images oder eine riskante Workload-Konfiguration. Unbefugte Benutzer können privilegierte Container als Taktik zur Rechteerweiterung starten, um sich zunächst Zugriff auf den Host zu verschaffen und ihn dann zu kompromittieren.

Die beobachtete Erstellung oder Änderung eines Containers wurde anhand des ML-Modells (Machine Learning) zur Erkennung von GuardDuty Anomalien als anomal identifiziert. Das ML-Modell bewertet alle Benutzer-API- und Container-Image-Aktivitäten innerhalb Ihres EKS-Clusters. Dieses ML-Modell identifiziert auch ungewöhnliche Ereignisse, die mit den von einem nicht autorisierten Benutzer verwendeten Techniken zusammenhängen. Das ML-Modell verfolgt mehrere Faktoren des API-Vorgangs, z. B. den Benutzer, der die Anfrage stellt, den Standort, von dem aus die Anfrage gestellt wurde, den verwendeten Benutzeragenten, in Ihrem Konto beobachtete Container-Images und den Namespace, den der Benutzer verwendet hat. Die ungewöhnlichen Details der API-Anfrage finden Sie im Bereich mit den Suchdetails in der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Wenn dieser Container-Start unerwartet erfolgt, wurden möglicherweise die Anmeldeinformationen der Benutzeridentität, die zum Starten des Containers verwendet wurde, kompromittiert. Sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

Falls Ihre AWS Anmeldeinformationen kompromittiert wurden, finden Sie weitere Informationen unterBehebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

Wenn dieser Container-Start erwartet wird, empfiehlt es sich, eine Unterdrückungsregel mit Filterkriterien zu verwenden, die auf dem

`resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`-Feld basieren. In den Filterkriterien sollte das `imagePrefix`-Feld dem in der Erkenntnis angegebenen Feld `imagePrefix` entsprechen. Weitere Informationen finden Sie unter Unterdrückungsregeln in GuardDuty.

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated

Eine sehr freizügige Rolle oder ClusterRole wurde auf ungewöhnliche Weise erstellt oder geändert.

Standard-Schweregrad: Niedrig

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein Kubernetes-Benutzer in Ihrem Amazon-EKS-Cluster einen anomale API-Vorgang zur Erstellung eines `Role` oder `ClusterRole` mit übermäßigen Berechtigungen aufgerufen hat. Akteure können die Rollenerstellung mit leistungsstarken Berechtigungen verwenden, um die Verwendung integrierter Administratorrollen zu vermeiden und so zu verhindern, dass sie entdeckt werden. Die übermäßigen Berechtigungen können zur Eskalation von Rechten, zur Ausführung von Remote-Code und möglicherweise zur Kontrolle über einen Namespace oder Cluster führen. Wenn dieses Verhalten nicht erwartet wird, deutet dies möglicherweise auf einen Konfigurationsfehler hin oder darauf, dass Ihre -Anmeldeinformationen kompromittiert wurden.

Die beobachtete API wurde anhand des ML-Modells (Machine Learning) zur Erkennung von GuardDuty Anomalien als anomal identifiziert. Das ML-Modell bewertet alle Benutzer-API-Aktivitäten innerhalb Ihres Amazon-EKS-Clusters und identifiziert anomale Ereignisse, die mit Techniken in Verbindung stehen, die von nicht autorisierten Benutzern verwendet werden. Das ML-Modell verfolgt mehrere Faktoren des API-Vorgangs, z. B. den Benutzer, der die Anfrage stellt, den Standort, von dem aus die Anfrage gestellt wurde, den verwendeten Benutzeragenten, in Ihrem Konto beobachtete Container-Images und den Namespace, den der Benutzer verwendet hat. Die ungewöhnlichen Details der API-Anfrage finden Sie im Bereich mit den Suchdetails in der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Prüfen Sie die in `Role` oder `ClusterRole` definierten Berechtigungen, um sicherzustellen, dass alle Berechtigungen benötigt werden, und halten Sie sich an die Grundsätze der geringsten Berechtigung. Wenn die Berechtigungen irrtümlich oder böswillig erteilt wurden, sollten Sie dem Benutzer den Zugriff entziehen und alle von einem Angreifer an Ihrem Cluster vorgenommenen

Änderungen rückgängig machen. Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

Falls Ihre AWS Anmeldeinformationen kompromittiert wurden, finden Sie weitere Informationen unterBehebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

Ein Benutzer hat seine Zugriffsberechtigungen auf ungewöhnliche Weise überprüft.

Standard-Schweregrad: Niedrig

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein Benutzer in Ihrem Kubernetes-Cluster erfolgreich geprüft hat, ob die bekannten mächtigen Berechtigungen, die zu privilegierter Eskalation und Remote-Codeausführung führen können, zulässig sind. Ein gängiger Befehl, der verwendet wird, um die Berechtigungen eines Benutzers zu überprüfen, ist beispielsweise `kubectl auth can-i`. Wenn dieses Verhalten nicht erwartet wird, deutet dies möglicherweise auf einen Konfigurationsfehler hin oder darauf, dass Ihre Anmeldeinformationen kompromittiert wurden.

Die beobachtete API wurde anhand des ML-Modells (Machine Learning) zur Erkennung von GuardDuty Anomalien als anomal identifiziert. Das ML-Modell bewertet alle Benutzer-API-Aktivitäten innerhalb Ihres Amazon-EKS-Clusters und identifiziert anomale Ereignisse, die mit Techniken in Verbindung stehen, die von nicht autorisierten Benutzern verwendet werden. Das ML-Modell verfolgt auch mehrere Faktoren des API-Vorgangs, z. B. den Benutzer, der die Anfrage stellt, den Standort, von dem aus die Anfrage gestellt wurde, die Überprüfung der Berechtigungen und den Namespace, den der Benutzer verwendet hat. Die ungewöhnlichen Details der API-Anfrage finden Sie im Bereich mit den Suchdetails in der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Prüfen Sie die dem Kubernetes-Benutzer erteilten Berechtigungen, um sicherzustellen, dass alle Berechtigungen benötigt werden. Wenn die Berechtigungen irrtümlich oder böswillig erteilt wurden, sollten Sie dem Benutzer den Zugriff entziehen und alle von einem Angreifer an Ihrem Cluster vorgenommenen Änderungen rückgängig machen. Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

Falls Ihre AWS Anmeldeinformationen kompromittiert wurden, finden Sie weitere Informationen unterBehebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

GuardDuty Findetypen für die Laufzeitüberwachung

Amazon GuardDuty generiert die folgenden Runtime Monitoring-Ergebnisse, um potenzielle Bedrohungen auf der Grundlage des Verhaltens auf Betriebssystemebene durch Amazon EC2-Hosts und Container in Ihren Amazon EKS-Clustern, Fargate- und Amazon ECS-Workloads sowie Amazon EC2-Instances aufzuzeigen.

> **Note**
>
> Die Erkenntnistypen der Laufzeit-Überwachung basieren auf den Laufzeit-Protokollen, die von Hosts gesammelt wurden. Die Protokolle enthalten Felder wie Dateipfade, die möglicherweise von einem böswilligen Akteur kontrolliert werden. Diese Felder sind auch in den GuardDuty Ergebnissen enthalten, um den Laufzeitkontext bereitzustellen. Wenn Sie Runtime Monitoring-Ergebnisse außerhalb der GuardDuty Konsole verarbeiten, müssen Sie die Ergebnisfelder bereinigen. Sie können z. B. Erkenntnisfelder HTML-kodieren, wenn Sie sie auf einer Webseite anzeigen.

Themen

- CryptoCurrency:Runtime/BitcoinTool.B
- Backdoor:Runtime/C&CActivity.B
- UnauthorizedAccess:Runtime/TorRelay
- UnauthorizedAccess:Runtime/TorClient
- Trojan:Runtime/BlackholeTraffic
- Trojan:Runtime/DropPoint
- CryptoCurrency:Runtime/BitcoinTool.B! DNS
- Backdoor:Runtime/C&CActivity.B! DNS
- Trojan:Runtime/BlackholeTraffic! DNS
- Trojan:Runtime/DropPoint! DNS
- Trojan:Runtime/DGADomainRequest.C! DNS
- Trojan:Runtime/DriveBySourceTraffic! DNS
- Trojan:Runtime/PhishingDomainRequest! DNS
- Impact:Runtime/AbusedDomainRequest.Reputation
- Impact:Runtime/BitcoinDomainRequest.Reputation

- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation
- UnauthorizedAccess:Runtime/MetadataDNSRebind
- Execution:Runtime/NewBinaryExecuted
- PrivilegeEscalation:Runtime/DockerSocketAccessed
- PrivilegeEscalation:Runtime/RuncContainerEscape
- PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified
- DefenseEvasion:Runtime/ProcessInjection.Proc
- DefenseEvasion:Runtime/ProcessInjection.Ptrace
- DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite
- Execution:Runtime/ReverseShell
- DefenseEvasion:Runtime/FilelessExecution
- Impact:Runtime/CryptoMinerExecuted
- Execution:Runtime/NewLibraryLoaded
- PrivilegeEscalation:Runtime/ContainerMountsHostDirectory
- PrivilegeEscalation:Runtime/UserfaultfdUsage
- Execution:Runtime/SuspiciousTool
- Execution:Runtime/SuspiciousCommand
- DefenseEvasion:Runtime/SuspiciousCommand
- DefenseEvasion:Runtime/PtraceAntiDebugging
- Execution:Runtime/MaliciousFileExecuted
- Execution:Runtime/MaliciousFileExecuted.Custom
- Execution:Runtime/SuspiciousShellCreated
- PrivilegeEscalation:Runtime/ElevationToRoot
- Discovery:Runtime/SuspiciousCommand
- Persistence:Runtime/SuspiciousCommand
- PrivilegeEscalation:Runtime/SuspiciousCommand
- DefenseEvasion:Runtime/KernelModuleLoaded
- Persistence:Runtime/SensitiveFileModified
- PrivilegeEscalation:Runtime/SensitiveFileModified

- DefenseEvasion:Runtime/SensitiveFileModified

CryptoCurrency:Runtime/BitcoinTool.B

Eine Amazon-EC2-Instance oder ein Container fragt eine IP-Adresse ab, die mit einer Aktivität in Zusammenhang mit einer Kryptowährung in Verbindung steht.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein Prozess, der auf der aufgeführten EC2-Instance oder einem Container in Ihrer AWS Umgebung ausgeführt wird, eine IP-Adresse abfragt, die mit einer kryptowährungsbezogenen Aktivität verknüpft ist. Bedrohungsakteure können versuchen, die Kontrolle über Datenverarbeitungsressourcen zu übernehmen, um sie böswillig für das unerlaubte Mining von Kryptowährungen umzuwidmen.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie in der GuardDuty Konsole im Ergebnisbereich unter Ressourcentyp nach. Zusätzliche Kontextinformationen, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn Sie diese EC2-Instance oder einen Container verwenden, um Kryptowährung zu minen oder zu verwalten, oder einer von beiden anderweitig in Blockchain-Aktivitäten involviert ist, könnte die CryptoCurrency:Runtime/BitcoinTool.B-Erkenntnis eine erwartete Aktivität für Ihre Umgebung darstellen. Wenn dies in Ihrer AWS Umgebung der Fall ist, empfehlen wir Ihnen, eine Unterdrückungsregel für dieses Ergebnis einzurichten. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Filterkriterium sollte das Attribut Erkenntnistyp mit dem Wert `CryptoCurrency:Runtime/BitcoinTool.B` verwenden. Das zweite Filterkriterium sollte die Instance-ID der Instance oder die Container-Image-ID des Containers sein, der an Aktivitäten im Zusammenhang mit Kryptowährungen oder Blockchain beteiligt ist. Weitere Informationen finden Sie unter Unterdrückungsregeln.

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

Backdoor:Runtime/C&CActivity.B

Eine Amazon-EC2-Instance oder ein Container fragt eine IP-Adresse ab, die mit einem bekannten Command-and-Control-Server verbunden ist.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein Prozess, der auf der aufgeführten EC2-Instance oder einem Container in Ihrer AWS Umgebung ausgeführt wird, eine IP-Adresse abfragt, die einem bekannten Command and Control (C&C) -Server zugeordnet ist. Die aufgeführte Instance oder der aufgeführte Container sind möglicherweise kompromittiert. Command-and-control-Server sind Computer, die Befehle an Mitglieder eines Botnets senden.

Ein Botnet ist eine Sammlung von mit dem Internet verbundenen Geräten, zu denen PCs, Server, mobile Geräte und Geräte des Internets der Dinge gehören können, die mit einem allgemeinen Typ von Malware infiziert sind und von dieser kontrolliert werden. Botnets dienen häufig zum Verteilen von Malware und zum Sammeln von sich widerrechtlich angeeigneten Informationen, wie z. B. Kreditkartennummern. Je nach Zweck und Struktur des Botnets kann der C&C-Server auch den Befehl erteilen, einen Distributed Denial of Service (DDoS)-Angriff zu starten.

> **Note**
>
> Wenn die abgefragte IP log4j-bezogen ist, enthalten die Felder der zugehörigen Erkenntnis die folgenden Werte:
>
> - `service.additionalInfo.threatListName = Amazon`
> - `service.additionalInfo.threatName = Log4j Related`

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie in der GuardDuty Konsole im Ergebnisbereich unter Ressourcentyp nach. Zusätzliche Kontextinformationen, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

UnauthorizedAccess:Runtime/TorRelay

Ihre Amazon-EC2-Instance oder Ihr Container stellt Verbindungen mit einem Tor-Netzwerk als Tor-Relays her.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein Prozess, der auf der aufgelisteten EC2-Instance oder einem Container in Ihrer AWS Umgebung läuft, Verbindungen zu einem Tor-Netzwerk auf eine Weise herstellt, die darauf hindeutet, dass es als Tor-Relay fungiert. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Tor-Relays erhöhen die Anonymität der Kommunikation, indem sie den möglicherweise illegalen Datenverkehr des Kunden von einem Tor-Relay zu einem anderen weiterleiten.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie in der GuardDuty Konsole im Ergebnisbereich unter Ressourcentyp nach. Zusätzliche Kontextinformationen, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

UnauthorizedAccess:Runtime/TorClient

Ihre Amazon-EC2-Instance oder ein Container stellt Verbindungen mit einem Tor Guard oder einem Authority-Knoten her.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein Prozess, der auf der aufgelisteten EC2-Instance oder einem Container in Ihrer AWS Umgebung läuft, Verbindungen zu einem Tor Guard- oder Authority-Knoten herstellt. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Tor Guards und Authority-Knoten fungieren als erste Gateways in ein Tor-Netzwerk. Dieser Datenverkehr kann darauf hinweisen, dass diese EC2-Instance oder der Container als Client in einem Tor-Netzwerk fungieren. Dieser Befund kann auf einen unbefugten Zugriff auf Ihre AWS Ressourcen hinweisen, mit der Absicht, die wahre Identität des Angreifers zu verbergen.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie in der GuardDuty Konsole im Ergebnisbereich unter Ressourcentyp nach. Zusätzliche Kontextinformationen, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

Trojan:Runtime/BlackholeTraffic

Eine Amazon-EC2-Instance oder ein Container versucht, mit einer IP-Adresse eines Remote-Hosts zu kommunizieren, der ein bekanntes schwarzes Loch ist.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein Prozess, der auf der aufgeführten EC2-Instance oder einem Container in Ihrer AWS Umgebung ausgeführt wird, möglicherweise gefährdet ist, weil er versucht, mit der IP-Adresse eines schwarzen Lochs (oder Sinkholes) zu kommunizieren. Schwarze Löcher sind Stellen im Netzwerk, an denen eingehender oder ausgehender Datenverkehr stillschweigend verworfen wird, ohne die Quelle darüber zu informieren, dass die Daten den vorgesehenen Empfänger nicht erreicht haben. Die IP-Adresse eines schwarzen Lochs gibt einen Hostcomputer an, der nicht ausgeführt wird, oder eine Adresse, der kein Host zugewiesen wurde.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie in der GuardDuty Konsole im Ergebnisbereich unter Ressourcentyp nach. Zusätzliche Kontextinformationen, einschließlich

Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

Trojan:Runtime/DropPoint

Eine Amazon-EC2-Instance oder ein Container versucht, mit einer IP-Adresse eines Remote-Hosts zu kommunizieren, von dem bekannt ist, dass er Anmeldeinformationen und andere mithilfe von Malware gestohlene Daten enthält.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein Prozess, der auf der aufgeführten EC2-Instance oder einem Container in Ihrer AWS Umgebung ausgeführt wird, versucht, mit der IP-Adresse eines Remote-Hosts zu kommunizieren, von dem bekannt ist, dass er Anmeldeinformationen und andere gestohlene Daten enthält, die von Malware erfasst wurden.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie in der GuardDuty Konsole im Ergebnisbereich unter Ressourcentyp nach. Zusätzliche Kontextinformationen, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

CryptoCurrency:Runtime/BitcoinTool.B! DNS

Eine Amazon EC2-Instance oder ein Container fragt einen Domainnamen ab, der mit Aktivitäten in Zusammenhang mit Kryptowährungen in Verbindung steht.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein Prozess, der auf der aufgeführten EC2-Instance oder einem Container in Ihrer AWS Umgebung ausgeführt wird, einen Domainnamen abfragt, der mit Bitcoin oder einer anderen kryptowährungsbezogenen Aktivität verknüpft ist. Bedrohungsakteure können versuchen, die Kontrolle über Datenverarbeitungsressourcen zu übernehmen, um sie böswillig für das unerlaubte Mining von Kryptowährungen umzuwidmen.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie in der GuardDuty Konsole im Ergebnisbereich unter Ressourcentyp nach. Zusätzliche Kontextinformationen, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn Sie diese EC2-Instance oder den Container verwenden, um Kryptowährung zu minen oder zu verwalten, oder diese Instance anderweitig an der Blockchain-Aktivität beteiligt ist, könnte diese CryptoCurrency:Runtime/BitcoinTool.B!DNS-Erkenntnis erwartete Aktivitäten für Ihre Umgebung repräsentieren. Wenn dies in Ihrer AWS Umgebung der Fall ist, empfehlen wir Ihnen, eine Unterdrückungsregel für dieses Ergebnis einzurichten. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Erkenntnistyp mit dem Wert `CryptoCurrency:Runtime/BitcoinTool.B!DNS` verwenden. Das zweite Filterkriterium sollte die Instance-ID der Instance oder die Container-Image-ID des Containers sein, der an Aktivitäten im Zusammenhang mit Kryptowährungen oder Blockchain beteiligt ist. Weitere Informationen finden Sie unter Unterdrückungsregeln.

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

Backdoor:Runtime/C&CActivity.B! DNS

Eine Amazon EC2-Instance oder ein Container fragt einen Domainamen ab, der einem bekannten Command-and-Control-Server zugeordnet wird.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein Prozess, der auf der aufgeführten EC2-Instance oder dem Container in Ihrer AWS Umgebung ausgeführt wird, einen Domainnamen abfragt, der einem bekannten Command and Control (C&C) -Server zugeordnet ist. Die aufgelistete EC2 Instance oder der aufgelistete Container sind möglicherweise kompromittiert. Command-and-control-Server sind Computer, die Befehle an Mitglieder eines Botnets senden.

Ein Botnet ist eine Sammlung von mit dem Internet verbundenen Geräten, zu denen PCs, Server, mobile Geräte und Geräte des Internets der Dinge gehören können, die mit einem allgemeinen Typ von Malware infiziert sind und von dieser kontrolliert werden. Botnets dienen häufig zum Verteilen von Malware und zum Sammeln von sich widerrechtlich angeeigneten Informationen, wie z. B. Kreditkartennummern. Je nach Zweck und Struktur des Botnets kann der C&C-Server auch den Befehl erteilen, einen Distributed Denial of Service (DDoS)-Angriff zu starten.

> **Note**
>
> Wenn der abgefragte Domainname mit log4j zu tun hat, enthalten die Felder der zugehörigen Erkenntnis die folgenden Werte:
>
> - `service.additionalInfo.threatListName = Amazon`
> - `service.additionalInfo.threatName = Log4j Related`

> **Note**
>
> Um zu testen, wie dieser Ergebnistyp GuardDuty generiert wird, können Sie von Ihrer Instance aus (unter `dig` Linux oder Windows) eine DNS-Anfrage `nslookup` für eine Testdomain stellen. `guarddutyc2activityb.com`

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie in der GuardDuty Konsole im Ergebnisbereich unter Ressourcentyp nach. Zusätzliche Kontextinformationen, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

Trojan:Runtime/BlackholeTraffic! DNS

Eine Amazon EC2-Instance oder ein Container fragt einen Domainnamen ab, der an eine IP-Adresse eines schwarzen Lochs weitergeleitet wird.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein Prozess, der auf der aufgeführten EC2-Instance oder dem Container in Ihrer AWS Umgebung ausgeführt wird, möglicherweise gefährdet ist, weil er einen Domainnamen abfragt, der an eine Black-Hole-IP-Adresse umgeleitet wird. Schwarze Löcher sind Stellen im Netzwerk, an denen eingehender oder ausgehender Datenverkehr stillschweigend verworfen wird, ohne die Quelle darüber zu informieren, dass die Daten den vorgesehenen Empfänger nicht erreicht haben.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie in der GuardDuty Konsole im Ergebnisbereich unter Ressourcentyp nach. Zusätzliche Kontextinformationen, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

Trojan:Runtime/DropPoint! DNS

Eine Amazon-EC2-Instance oder ein Container fragt einen Domainnamen eines Remote-Hosts ab, von dem bekannt ist, dass er Anmeldeinformationen und andere mithilfe von Malware gestohlene Daten enthält.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein Prozess, der auf der aufgeführten EC2-Instance oder einem Container in Ihrer AWS Umgebung ausgeführt wird, den Domainnamen eines Remote-

Hosts abfragt, von dem bekannt ist, dass er Anmeldeinformationen und andere gestohlene Daten enthält, die von Malware erfasst wurden.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie in der GuardDuty Konsole im Ergebnisbereich unter Ressourcentyp nach. Zusätzliche Kontextinformationen, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

Trojan:Runtime/DGADomainRequest.C! DNS

Eine Amazon-EC2-Instance oder ein Container fragt algorithmisch generierte Domains ab. Solche Domains werden häufig von Malware genutzt und können auf eine kompromittierte EC2-Instance oder Container hinweisen.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein Prozess, der auf der aufgeführten EC2-Instance oder dem Container in Ihrer AWS Umgebung ausgeführt wird, versucht, Domänen mit dem Domaingenerierungsalgorithmus (DGA) abzufragen. Ihre Ressource wurde möglicherweise kompromittiert.

DGAs werden verwendet, um in regelmäßigen Abständen eine große Anzahl an Domainnamen zu generieren, die als Rendezvous Points mit ihren Command-and-Control (C&C)-Servern verwendet werden können. Command-and-Control-Server sind Computer, die Befehle an die Mitglieder eines Botnets senden. Hierbei handelt es sich um eine Ansammlung von mit dem Internet verbundenen Geräten, die infiziert sind und von einer gängigen Malware kontrolliert werden. Die große Anzahl potenzieller Rendezvous Points erschwert ein effektives Stilllegen von Botnets, da infizierte Computer versuchen, einige dieser Domainnamen täglich zu kontaktieren, um Updates oder Befehle zu erhalten.

> **Note**
>
> Dieses Ergebnis basiert auf bekannten DGA-Domänen aus GuardDuty Threat Intelligence-Feeds.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie in der GuardDuty Konsole im Ergebnisbereich unter Ressourcentyp nach. Zusätzliche Kontextinformationen, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

Trojan:Runtime/DriveBySourceTraffic! DNS

Eine Amazon EC2-Instance oder ein Container fragt den Domainnamen eines Remote-Hosts ab, der eine bekannte Quelle von Drive-By Download-Angriffen ist.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein Prozess, der auf der aufgeführten EC2-Instance oder dem Container in Ihrer AWS Umgebung ausgeführt wird, möglicherweise gefährdet ist, weil er den Domainnamen eines Remote-Hosts abfragt, der eine bekannte Quelle für Drive-by-Download-Angriffe ist. Hierbei handelt es sich um unbeabsichtigte Downloads von Computersoftware aus dem Internet, die eine automatische Installation von Viren, Spyware oder Malware auslösen kann.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie in der GuardDuty Konsole im Ergebnisbereich unter Ressourcentyp nach. Zusätzliche Kontextinformationen, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

Trojan:Runtime/PhishingDomainRequest! DNS

Eine Amazon-EC2-Instance oder ein Container fragt Domains ab, die an Phishing-Angriffen beteiligt sind.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein Prozess, der auf der aufgeführten EC2-Instance oder einem Container in Ihrer AWS Umgebung ausgeführt wird, versucht, eine Domain abzufragen, die an Phishing-Angriffen beteiligt ist. Phishing-Domains werden von jemandem eingerichtet, der sich als rechtmäßige Institution ausgibt, um Personen dazu zu bringen, sensible Daten bereitzustellen, wie beispielsweise personenbezogene Informationen, Bank- und Kreditkartendaten oder Passwörter. Ihre EC2-Instance oder der Container versucht möglicherweise, sensible Daten abzurufen, die auf einer Phishing-Website gespeichert sind, oder versucht möglicherweise, eine Phishing-Website einzurichten. Die EC2-Instance oder der Container sind möglicherweise kompromittiert.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie in der GuardDuty Konsole im Ergebnisbereich unter Ressourcentyp nach. Zusätzliche Kontextinformationen, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

Impact:Runtime/AbusedDomainRequest.Reputation

Eine Amazon-EC2-Instance oder ein Container fragt einen Domainnamen mit niedriger Reputation ab, der mit bekanntermaßen missbrauchten Domains verknüpft ist.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein Prozess, der auf der aufgeführten EC2-Instance oder dem Container in Ihrer AWS Umgebung ausgeführt wird, einen Domainnamen mit niedriger Reputation abfragt, der mit bekanntermaßen missbrauchten Domänen oder IP-Adressen verknüpft ist. Beispiele für missbrauchte Domains sind Top-Level-Domainnamen (TLDs) und Second-Level-Domainnamen (2LDs), die kostenlose Subdomain-Registrierungen bieten, sowie dynamische DNS-Anbieter. Bedrohungsakteure nutzen diese Services in der Regel, um Domains kostenlos oder zu geringen Kosten zu registrieren. Bei Domains mit geringer Reputation in dieser Kategorie kann es sich auch um abgelaufene Domains handeln, die auf die Parking-IP-Adresse eines Registrars zurückgehen und daher möglicherweise nicht mehr aktiv sind. Bei einer Parking-IP leitet ein Registrar den Verkehr für Domains weiter, die mit keinem Service verknüpft wurden. Die aufgelistete Amazon-EC2-Instance oder der Container können kompromittiert sein, da Bedrohungsakteure diese Registrare oder Services häufig für C&C und die Verbreitung von Malware nutzen.

Domains mit niedriger Reputation basieren auf einem Reputations-Punkte-Modell. Dieses Modell bewertet und bewertet die Eigenschaften einer Domain, um zu ermitteln, ob es sich um eine bösartige Domain handeln könnte.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie in der GuardDuty Konsole im Ergebnisbereich unter Ressourcentyp nach. Zusätzliche Kontextinformationen, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

Impact:Runtime/BitcoinDomainRequest.Reputation

Eine Amazon-EC2-Instance oder ein Container fragt einen Domainnamen ab, der mit einer Aktivität in Zusammenhang mit einer Kryptowährung in Verbindung steht.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein Prozess, der auf der aufgeführten EC2-Instance oder dem Container in Ihrer AWS Umgebung ausgeführt wird, einen Domainnamen mit niedriger Reputation abfragt, der mit Bitcoin oder anderen kryptowährungsbezogenen Aktivitäten in Verbindung steht. Bedrohungsakteure können versuchen, die Kontrolle über Datenverarbeitungsressourcen zu übernehmen, um sie böswillig für das unerlaubte Mining von Kryptowährungen umzuwidmen.

Domains mit niedriger Reputation basieren auf einem Reputations-Punkte-Modell. Dieses Modell bewertet und bewertet die Eigenschaften einer Domain, um zu ermitteln, ob es sich um eine bösartige Domain handeln könnte.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie in der GuardDuty Konsole im Ergebnisbereich unter Ressourcentyp nach. Zusätzliche Kontextinformationen, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn Sie diese EC2-Instance oder den Container verwenden, um Kryptowährung zu minen oder zu verwalten, oder diese Instance anderweitig an Blockchain-Aktivitäten beteiligt ist, könnte diese Erkenntnis erwartete Aktivitäten für Ihre Umgebung repräsentieren. Wenn dies in Ihrer AWS Umgebung der Fall ist, empfehlen wir Ihnen, eine Unterdrückungsregel für dieses Ergebnis einzurichten. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Filterkriterium sollte das Attribut Erkenntnistyp mit dem Wert `Impact:Runtime/BitcoinDomainRequest.Reputation` verwenden. Das zweite Filterkriterium sollte die Instance-ID der Instance oder die Container-Image-ID des Containers sein, der an Aktivitäten im Zusammenhang mit Kryptowährung oder Blockchain beteiligt ist. Weitere Informationen finden Sie unter Unterdrückungsregeln.

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

Impact:Runtime/MaliciousDomainRequest.Reputation

Eine Amazon-EC2-Instance oder ein Container fragt eine Domain mit niedriger Reputation ab, die mit bekannten bösartigen Domains verknüpft ist.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein Prozess, der auf der aufgeführten EC2-Instance oder dem Container in Ihrer AWS Umgebung ausgeführt wird, einen Domainnamen mit niedriger Reputation abfragt, der mit bekannten bösartigen Domänen oder IP-Adressen verknüpft ist. Beispielsweise können Domains mit einer bekannten Sinkhole-IP-Adresse verknüpft sein. Sinkhole-Domains sind Domains, die zuvor von einem Bedrohungsakteur kontrolliert wurden, und Anfragen an sie können darauf hinweisen, dass die Instance kompromittiert wurde. Diese Domains können auch mit bekannten böswilligen Kampagnen oder Algorithmen zur Domain-Generierung korreliert sein.

Domains mit niedriger Reputation basieren auf einem Reputations-Punkte-Modell. Dieses Modell bewertet und bewertet die Eigenschaften einer Domain, um zu ermitteln, ob es sich um eine bösartige Domain handeln könnte.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie in der GuardDuty Konsole im Ergebnisbereich unter Ressourcentyp nach. Zusätzliche Kontextinformationen, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

Impact:Runtime/SuspiciousDomainRequest.Reputation

Eine Amazon-EC2-Instance oder ein Container fragt einen Domainnamen mit geringer Reputation ab, der aufgrund seines Alters oder seiner geringen Beliebtheit verdächtig ist.

Standard-Schweregrad: Niedrig

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein Prozess, der auf der aufgeführten EC2-Instance oder dem Container in Ihrer AWS Umgebung ausgeführt wird, einen Domainnamen mit niedriger Reputation abfragt, von dem vermutet wird, dass er bösartig ist. Die beobachteten Merkmale dieser Domäne stimmten mit den zuvor beobachteten bösartigen Domänen überein. Unser Reputationsmodell war jedoch nicht in der Lage, es definitiv mit einer bekannten Bedrohung in

Verbindung zu bringen. Diese Domains werden in der Regel neu beobachtet oder erhalten nur wenig Datenverkehr.

Domains mit niedriger Reputation basieren auf einem Reputations-Punkte-Modell. Dieses Modell bewertet und bewertet die Eigenschaften einer Domain, um zu ermitteln, ob es sich um eine bösartige Domain handeln könnte.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie in der GuardDuty Konsole im Ergebnisbereich unter Ressourcentyp nach. Zusätzliche Kontextinformationen, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

UnauthorizedAccess:Runtime/MetadataDNSRebind

Eine Amazon-EC2-Instance oder ein Container führen DNS-Lookups durch, die in den Instance-Metadatenservice aufgelöst werden.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

> **Note**
>
> Derzeit wird dieser Ergebnistyp nur für die AMD64-Architektur unterstützt.

Dieses Ergebnis informiert Sie darüber, dass ein Prozess, der auf der aufgeführten EC2-Instance oder einem Container in Ihrer AWS Umgebung ausgeführt wird, eine Domain abfragt, die in die EC2-Metadaten-IP-Adresse (169.254.169.254) aufgelöst wird. Eine solche DNS-Abfrage kann darauf hinweisen, dass die Instance das Ziel einer DNS-Neubindung-Technik ist. Diese Technik kann verwendet werden, um Metadaten von einer EC2-Instance abzurufen, einschließlich der mit der Instance verknüpften IAM-Anmeldeinformationen.

Bei der DNS-Neubindung wird eine Anwendung, die auf der EC2-Instance läuft, dazu gebracht, Rückgabedaten von einer URL zu laden, wobei der Domainname in der URL in die IP-Adresse der EC2-Metadaten (`169.254.169.254`) aufgelöst wird. Dies bewirkt, dass die Anwendung auf EC2-Metadaten zugreift und sie möglicherweise für den Angreifer verfügbar macht.

Der Zugriff auf EC2-Metadaten mit DNS-Neubindung ist nur möglich, wenn auf der EC2-Instance eine anfällige Anwendung ausgeführt wird, die das Einfügen von URLs ermöglicht, oder wenn ein menschlicher Benutzer in einem Webbrowser, der auf der EC2-Instance ausgeführt wird, auf die URL zugreift.

Der Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. GuardDuty Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie in der GuardDuty Konsole im Ergebnisbereich unter Ressourcentyp nach. Zusätzliche Kontextinformationen, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Prüfen Sie als Reaktion auf diese Erkenntnis, ob auf der EC2-Instance oder dem Container eine anfällige Anwendung ausgeführt wird, oder ob ein menschlicher Benutzer über einen Browser auf die in der Erkenntnis angegebene Domain zugegriffen hat. Wenn die Ursache eine anfällige Anwendung ist, beheben Sie die Schwachstelle. Wenn ein Benutzer die identifizierte Domain aufgerufen hat, blockieren Sie die Domain oder verhindern Sie, dass Benutzer darauf zugreifen. Wenn Sie in dieser Erkenntnis einen Zusammenhang mit einem der obigen Fälle feststellen, sollten Sie die mit der EC2-Instance verknüpfte Sitzung widerrufen.

Einige AWS Kunden ordnen die Metadaten-IP-Adresse absichtlich einem Domainnamen auf ihren autoritativen DNS-Servern zu. Wenn dies in Ihrer -Umgebung der Fall ist, empfehlen wir, für diese Erkenntnis eine Unterdrückungsregel festzulegen. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Filterkriterium sollte das Attribut Erkenntnistyp mit dem Wert `UnauthorizedAccess:Runtime/MetadataDNSRebind` verwenden. Das zweite Filterkriterium sollte die DNS-Anforderungs-Domain oder die Container-Image-ID des Containers sein. Das zweite Filterkriterium sollte die DNS-Anforderungs-Domain sein, und der Wert sollte mit der Domain übereinstimmen, die Sie der Metadaten-IP-Adresse zugeordnet haben (`169.254.169.254`). Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln.

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

Execution:Runtime/NewBinaryExecuted

Eine neu erstellte oder kürzlich geänderte Binärdatei in einem Container wurde ausgeführt.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass eine neu erstellte oder kürzlich geänderte Binärdatei in einem Container ausgeführt wurde. Es ist eine bewährte Methode, Container zur Laufzeit unveränderlich zu halten. Binärdateien, Skripten oder Bibliotheken sollten während der Lebensdauer des Containers nicht erstellt oder geändert werden. Dieses Verhalten weist darauf hin, dass ein böswilliger Akteur Zugriff auf den Container erhalten, Malware oder andere Software heruntergeladen und im Rahmen der potenziellen Kompromittierung ausgeführt hat. Obwohl diese Art von Aktivität ein Hinweis auf eine Kompromittierung sein könnte, ist sie auch ein weit verbreitetes Nutzungsmuster. GuardDuty Verwendet daher Mechanismen, um verdächtige Fälle dieser Aktivität zu identifizieren, und generiert diesen Ergebnistyp nur für verdächtige Fälle.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie in der GuardDuty Konsole im Ergebnisbereich unter Ressourcentyp nach. Um den Änderungsprozess und die neue Binärdatei zu identifizieren, sehen Sie sich die Prozessdetails zum Ändern und die Prozessdetails an

Die Einzelheiten des Änderungsprozesses sind im `service.runtimeDetails.context.modifyingProcess` JSON-Feld für die Suche oder im Bereich „Findungsdetails“ unter „Prozess ändern“ enthalten. Bei diesem Ergebnistyp erfolgt der Änderungsvorgang entsprechend dem `service.runtimeDetails.context.modifyingProcess.executablePath` JSON-Feld für die Suche oder als Teil des Änderungsprozesses im Bereich mit den Suchdetails. `/usr/bin/dpkg`

Die Details der ausgeführten neuen oder geänderten Binärdatei sind in `service.runtimeDetails.process` der JSON-Datei für die Suche oder im Abschnitt „Prozess“ unter „Laufzeitdetails“ enthalten. Für diesen Findetyp ist die neue oder geänderte Binärdatei`/usr/bin/python3.8`, wie im Feld `service.runtimeDetails.process.executablePath` (Ausführbarer Pfad) angegeben.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

PrivilegeEscalation:Runtime/DockerSocketAccessed

Ein Prozess in einem Container kommuniziert über den Docker-Socket mit dem Docker-Daemon.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Der Docker-Socket ist ein Unix-Domain-Socket, den Docker-Daemon (`dockerd`) verwendet, um mit seinen Clients zu kommunizieren. Ein Client kann verschiedene Aktionen ausführen, z. B. das Erstellen von Containern, indem er über den Docker-Socket mit dem Docker-Daemon kommuniziert. Es ist verdächtig, dass ein Container-Prozess auf den Docker-Socket zugreift. Ein Container-Prozess kann dem Container entkommen und Zugriff auf Host-Ebene erhalten, indem er mit dem Docker-Socket kommuniziert und einen privilegierten Container erstellt.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie in der GuardDuty Konsole im Ergebnisbereich unter Ressourcentyp nach. Zusätzliche Kontextinformationen, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

PrivilegeEscalation:Runtime/RuncContainerEscape

Ein Container-Escape-Versuch über runC wurde erkannt.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

RunC ist die Low-Level-Container-Runtime, die High-Level-Container-Runtimes wie Docker und Containerd verwenden, um Container zu erzeugen und auszuführen. RunC wird immer mit Root-Rechten ausgeführt, da es die Low-Level-Aufgabe der Erstellung eines Containers ausführen muss. Ein Bedrohungsakteur kann sich Zugriff auf Host-Ebene verschaffen, indem er eine Sicherheitslücke in der RunC-Binärdatei entweder modifiziert oder ausnutzt.

Dieses Ergebnis erkennt Änderungen an der RunC-Binärdatei und potenzielle Versuche, die folgenden RunC-Sicherheitslücken auszunutzen:

- CVE-2019-5736— CVE-2019-5736 Bei der Ausnutzung von wird die RunC-Binärdatei aus einem Container heraus überschrieben. Dieses Ergebnis wird aufgerufen, wenn die RunC-Binärdatei durch einen Prozess in einem Container geändert wird.
- CVE-2024-21626— CVE-2024-21626 Bei der Ausnutzung von wird das aktuelle Arbeitsverzeichnis (CWD) oder ein Container auf einen offenen Dateideskriptor gesetzt. `/proc/self/fd/`*`FileDescriptor`* Dieses Ergebnis wird ausgelöst, wenn ein Container-Prozess erkannt wird, unter dem sich ein aktuelles Arbeitsverzeichnis `/proc/self/fd/` befindet, zum Beispiel. `/proc/self/fd/7`

Diese Erkenntnis könnte darauf hindeuten, dass ein böswilliger Akteur versucht hat, einen der folgenden Containertypen auszunutzen:

- Ein neuer Container mit einem vom Angreifer kontrollierten Image.
- Ein vorhandener Container, auf den der Akteur mit Schreibberechtigungen auf der runC-Binärdatei auf Host-Ebene zugreifen konnte.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie in der GuardDuty Konsole im Ergebnisbereich unter Ressourcentyp nach.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified

Ein Container-Escape-Versuch über den CGroups-Release-Agent wurde erkannt.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Diese Erkenntnis informiert Sie darüber, dass ein Versuch erkannt wurde, eine Release-Agent-Datei für eine Kontrollgruppe (Cgroup) zu ändern. Linux verwendet Kontrollgruppen (Cgroups), um die Ressourcennutzung einer Reihe von Prozessen einzuschränken, zu berücksichtigen und zu isolieren. Jede Cgroup hat eine Release-Agent-Datei (`release_agent`), ein Skript, das Linux ausführt, wenn ein Prozess innerhalb der Cgroup beendet wird. Die Release-Agent-Datei wird immer auf Host-Ebene ausgeführt. Ein Bedrohungsakteur in einem Container kann zum Host entkommen, indem er beliebige Befehle in die Release-Agent-Datei schreibt, die zu einer Cgroup gehört. Wenn ein Prozess innerhalb dieser Cgroup beendet wird, werden die vom Akteur geschriebenen Befehle ausgeführt.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie in der GuardDuty Konsole im Ergebnisbereich unter Ressourcentyp nach.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

DefenseEvasion:Runtime/ProcessInjection.Proc

In einem Container oder einer Amazon-EC2-Instance wurde eine Prozessinjektion mithilfe des proc-Dateisystems erkannt.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Bei der Prozessinjektion handelt es sich um eine Technik, mit der Bedrohungsakteure Code in Prozesse einschleusen, um Schutzmaßnahmen zu umgehen und möglicherweise Rechte zu erweitern. Das proc-Dateisystem (procfs) ist ein spezielles Dateisystem in Linux, das den virtuellen Speicher eines Prozesses als Datei darstellt. Der Pfad dieser Datei ist `/proc/PID/mem`, wobei `PID`

die eindeutige ID des Prozesses ist. Ein Bedrohungsakteur kann in diese Datei schreiben, um Code in den Prozess einzuschleusen. Diese Erkenntnis identifiziert potenzielle Versuche, in diese Datei zu schreiben.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie in der GuardDuty Konsole im Ergebnisbereich unter Ressourcentyp nach. Zusätzliche Kontextinformationen, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität unerwartet ist, wurde Ihr Ressourcentyp möglicherweise kompromittiert. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

DefenseEvasion:Runtime/ProcessInjection.Ptrace

In einem Container oder einer Amazon-EC2-Instance wurde eine Prozessinjektion mithilfe des ptrace-Systemaufrufs erkannt.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Bei der Prozessinjektion handelt es sich um eine Technik, mit der Bedrohungsakteure Code in Prozesse einschleusen, um Schutzmaßnahmen zu umgehen und möglicherweise Rechte zu erweitern. Ein Prozess kann den ptrace-Systemaufruf verwenden, um Code in einen anderen Prozess einzuschleusen. Diese Erkenntnis identifiziert einen möglichen Versuch, mithilfe des Systemaufrufs ptrace Code in einen Prozess einzuschleusen.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie in der GuardDuty Konsole im Ergebnisbereich unter Ressourcentyp nach. Zusätzliche Kontextinformationen, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität unerwartet ist, wurde Ihr Ressourcentyp möglicherweise kompromittiert. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite

In einem Container oder einer Amazon-EC2-Instance wurde eine Prozessinjektion durch direktes Schreiben in den virtuellen Speicher erkannt.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Bei der Prozessinjektion handelt es sich um eine Technik, mit der Bedrohungsakteure Code in Prozesse einschleusen, um Schutzmaßnahmen zu umgehen und möglicherweise Rechte zu erweitern. Ein Prozess kann einen Systemaufruf wie `process_vm_writev` verwenden, um Code direkt in den virtuellen Speicher eines anderen Prozesses einzuschleusen. Diese Erkenntnis identifiziert einen möglichen Versuch, mithilfe eines Systemaufrufs Code in den virtuellen Speicher eines Prozesses einzuschleusen.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie in der GuardDuty Konsole im Ergebnisbereich unter Ressourcentyp nach. Zusätzliche Kontextinformationen, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität unerwartet ist, wurde Ihr Ressourcentyp möglicherweise kompromittiert. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

Execution:Runtime/ReverseShell

Ein Prozess in einem Container oder einer Amazon-EC2-Instance hat eine Reverse-Shell erstellt.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Eine Reverse-Shell ist eine Shell-Sitzung, die auf einer Verbindung erstellt wird, die vom Zielhost zum Host des Akteurs initiiert wird. Dies ist das Gegenteil einer normalen Shell, die vom Host des Akteurs

zum Host des Ziels initiiert wird. Bedrohungsakteure erstellen eine Reverse-Shell, um Befehle auf dem Ziel auszuführen, nachdem sie sich den ersten Zugriff auf das Ziel verschafft haben. Dieser Befund identifiziert potenziell verdächtige Reverse-Shell-Verbindungen.

GuardDuty untersucht die zugehörige Laufzeitaktivität und den zugehörigen Kontext und generiert diesen Ergebnistyp nur, wenn sich herausstellt, dass die zugehörige Aktivität und der Kontext ungewöhnlich oder verdächtig sind. Zusätzliche Kontextinformationen, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Der GuardDuty Security Agent überwacht Ereignisse aus mehreren Quellen. Um die betroffene Ressource zu identifizieren, sehen Sie in den Suchdetails in der GuardDuty Konsole den Ressourcentyp an. Wenn diese Aktivität unerwartet ist, wurde Ihr Ressourcentyp möglicherweise kompromittiert. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

DefenseEvasion:Runtime/FilelessExecution

Ein Prozess in einem Container oder einer Amazon-EC2-Instance führt Code aus dem Speicher aus.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Diese Erkenntnis informiert Sie darüber, wenn ein Prozess mit einer im Speicher befindlichen ausführbaren Datei auf der Festplatte ausgeführt wird. Dabei handelt es sich um eine gängige Technik zur Umgehung von Schutzmaßnahmen, bei der verhindert wird, dass die schädliche ausführbare Datei auf die Festplatte geschrieben wird, um der Erkennung durch Dateisystem-Scans zu entgehen. Diese Technik wird zwar von Schadsoftware verwendet, hat aber auch einige legitime Anwendungsfälle. Eines der Beispiele ist ein Just-in-Time-Compiler (JIT), der kompilierten Code in den Speicher schreibt und ihn aus dem Speicher ausführt.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie in der GuardDuty Konsole im Ergebnisbereich unter Ressourcentyp nach. Zusätzliche Kontextinformationen, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

Impact:Runtime/CryptoMinerExecuted

Ein Container oder eine Amazon-EC2-Instance führt eine Binärdatei aus, die mit einer Cryptocurrency-Mining-Aktivität verknüpft ist.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein Prozess, der auf der aufgeführten EC2-Instance oder dem aufgelisteten EC2-Container in Ihrer AWS Umgebung ausgeführt wird, eine Binärdatei ausführt, die mit einer Cryptocurrency-Mining-Aktivität verknüpft ist. Bedrohungsakteure können versuchen, die Kontrolle über Datenverarbeitungsressourcen zu übernehmen, um sie böswillig für das unerlaubte Mining von Kryptowährungen umzuwidmen.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie in der GuardDuty Konsole im Ergebnisbereich unter Ressourcentyp nach. Zusätzliche Kontextinformationen, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Der GuardDuty Runtime Agent überwacht Ereignisse von mehreren Ressourcen aus. Um die betroffene Ressource zu identifizieren, sehen Sie in den Ergebnisdetails in der GuardDuty Konsole unter Ressourcentyp nachKorrigieren von Erkenntnissen der Laufzeitüberwachung.

Execution:Runtime/NewLibraryLoaded

Eine neu erstellte oder kürzlich geänderte Bibliothek wurde von einem Prozess in einen Container geladen.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Diese Erkenntnis informiert Sie darüber, dass eine Bibliothek während der Laufzeit in einem Container erstellt oder geändert und von einem Prozess geladen wurde, der innerhalb des Containers ausgeführt wird. Es ist eine bewährte Methode, Container zur Laufzeit unveränderlich zu halten. Binärdateien, Skripten oder Bibliotheken sollten während der Lebensdauer des Containers nicht erstellt oder geändert werden. Das Laden einer neu erstellten oder geänderten Bibliothek in einen Container kann auf verdächtige Aktivitäten hinweisen. Dieses Verhalten weist auf einen böswilligen Akteur hin, der sich Zugriff auf den Container verschafft und im Rahmen der potenziellen Sicherheitslücke Malware oder andere Software heruntergeladen und ausgeführt hat. Obwohl diese Art von Aktivität ein Hinweis auf eine Kompromittierung sein könnte, ist sie auch ein weit verbreitetes Nutzungsmuster. GuardDuty Verwendet daher Mechanismen, um verdächtige Fälle dieser Aktivität zu identifizieren, und generiert diesen Ergebnistyp nur für verdächtige Fälle.

Der GuardDuty Runtime Agent überwacht Ereignisse von mehreren Ressourcen aus. Um die betroffene Ressource zu identifizieren, sehen Sie in den Ergebnisdetails in der GuardDuty Konsole den Ressourcentyp an. Zusätzliche Informationen zum Kontext, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

PrivilegeEscalation:Runtime/ContainerMountsHostDirectory

Ein Prozess in einem Container hat zur Laufzeit ein Host-Dateisystem gemountet.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Bei mehreren Techniken zur Container-Escape-Methode wird zur Laufzeit ein Host-Dateisystem in einem Container gemountet. Diese Erkenntnis informiert Sie darüber, dass ein Prozess in einem Container möglicherweise versucht hat, ein Host-Dateisystem zu mounten, was auf einen Fluchtversuch zum Host hindeuten kann.

Der GuardDuty Runtime Agent überwacht Ereignisse von mehreren Ressourcen aus. Um die betroffene Ressource zu identifizieren, sehen Sie in den Ergebnisdetails in der GuardDuty Konsole

den Ressourcentyp an. Zusätzliche Informationen zum Kontext, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

PrivilegeEscalation:Runtime/UserfaultfdUsage

Ein Prozess verwendete userfaultfd-Systemaufrufe, um Seitenfehler im Benutzerbereich zu behandeln.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Typischerweise werden Seitenfehler vom Kernel im Kernel-Space behandelt. Ein `userfaultfd`-Systemaufruf ermöglicht es einem Prozess jedoch, Seitenfehler in einem Dateisystem in der Benutzerumgebung zu behandeln. Dies ist eine nützliches Feature, die die Implementierung von Dateisystemen in der Benutzerumgebung ermöglicht. Andererseits kann sie auch von einem potenziell bösartigen Prozess verwendet werden, um den Kernel von der Benutzerumgebung aus zu unterbrechen. Das Unterbrechen des Kernels mithilfe eines `userfaultfd`-Systemaufrufs ist eine gängige Ausnutzungstechnik, um Race-Fenster zu verlängern, während die Kernel-Race-Bedingungen ausgenutzt werden. Die Verwendung von `userfaultfd` kann auf verdächtige Aktivitäten auf der Amazon Elastic Compute Cloud (Amazon EC2)-Instance hinweisen.

Der GuardDuty Runtime Agent überwacht Ereignisse von mehreren Ressourcen aus. Um die betroffene Ressource zu identifizieren, sehen Sie in den Ergebnisdetails in der GuardDuty Konsole den Ressourcentyp an. Zusätzliche Informationen zum Kontext, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

Execution:Runtime/SuspiciousTool

Ein Container oder eine Amazon-EC2-Instance führt eine Binärdatei oder ein Skript aus, das häufig in offensiven Sicherheitsszenarien wie Pentesting-Angriffen verwendet wird.

Standard-Schweregrad: Variabel

Der Schweregrad dieses Befundes kann entweder hoch oder niedrig sein, je nachdem, ob das erkannte verdächtige Tool als doppelter Verwendungszweck eingestuft wird oder ob es ausschließlich für anstößige Zwecke bestimmt ist.

- Feature: Laufzeit-Überwachung

Dieser Befund informiert Sie darüber, dass ein verdächtiges Tool auf einer EC2-Instance oder einem EC2-Container in Ihrer AWS Umgebung ausgeführt wurde. Dazu gehören Tools, die bei Pentesting-Projekten verwendet werden, auch bekannt als Backdoor-Tools, Netzwerkscanner und Netzwerk-Sniffer. Alle diese Tools können in harmlosen Zusammenhängen eingesetzt werden, werden aber auch häufig von Bedrohungsakteuren mit böswilliger Absicht verwendet. Die Beobachtung anstößiger Sicherheitstools könnte darauf hindeuten, dass die zugehörige EC2-Instance oder der zugehörige EC2-Container kompromittiert wurde.

GuardDuty untersucht die zugehörigen Laufzeitaktivitäten und den zugehörigen Kontext, sodass dieses Ergebnis nur generiert wird, wenn die zugehörige Aktivität und der Kontext potenziell verdächtig sind.

Der GuardDuty Runtime Agent überwacht Ereignisse von mehreren Ressourcen aus. Um die betroffene Ressource zu identifizieren, sehen Sie in den Ergebnisdetails in der GuardDuty Konsole den Ressourcentyp an. Falls zutreffend, ist im Ergebnis zusätzlicher Kontext, einschließlich Informationen zum Prozess und zur Prozessherkunft, für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

Execution:Runtime/SuspiciousCommand

Ein verdächtiger Befehl wurde auf einer Amazon-EC2-Instance oder in einem Container ausgeführt. Dies weist auf eine Kompromittierung hin.

Standard-Schweregrad: Variabel

Je nach Auswirkung des beobachteten bösartigen Musters kann der Schweregrad dieses Erkenntnistyps entweder niedrig, mittel oder hoch sein.

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein verdächtiger Befehl ausgeführt wurde, und weist darauf hin, dass eine Amazon EC2-Instance oder ein Container in Ihrer AWS Umgebung kompromittiert wurde. Dies kann bedeuten, dass entweder eine Datei aus einer verdächtigen Quelle heruntergeladen und dann ausgeführt wurde oder dass ein laufender Prozess in seiner Befehlszeile ein bekanntes bösartiges Muster zeigt. Dies weist außerdem darauf hin, dass Malware auf dem System ausgeführt wird.

GuardDuty untersucht die zugehörige Laufzeitaktivität und den zugehörigen Kontext, sodass dieses Ergebnis nur generiert wird, wenn die zugehörige Aktivität und der Kontext potenziell verdächtig sind.

Der GuardDuty Runtime Agent überwacht Ereignisse von mehreren Ressourcen aus. Um die betroffene Ressource zu identifizieren, sehen Sie in den Ergebnisdetails in der GuardDuty Konsole den Ressourcentyp an. Falls zutreffend, ist im Ergebnis zusätzlicher Kontext, einschließlich Informationen zum Prozess und zur Prozessherkunft, für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

> **Note**
>
> Befehlszeilenargumente für die Verarbeitung können vertrauliche Daten enthalten. Zum Schutz vertraulicher Daten enthalten die Ergebnisse der GuardDuty Laufzeitüberwachung keine vollständigen Befehlszeilenargumente. Zeigt stattdessen ein repräsentatives Beispiel `Service.RuntimeDetails.Context.CommandLineExample` für das Befehlszeilenmuster, das das Ergebnis generiert hat.

DefenseEvasion:Runtime/SuspiciousCommand

Ein Befehl wurde auf der aufgelisteten Amazon-EC2-Instance oder in einem Container ausgeführt. Damit wird versucht, einen Linux-Abwehrmechanismus wie eine Firewall oder wichtige Systemdienste zu ändern oder zu deaktivieren.

Standard-Schweregrad: Variabel

Je nachdem, welcher Abwehrmechanismus verändert oder deaktiviert wurde, kann der Schweregrad dieses Erkenntnistyps entweder hoch, mittel oder niedrig sein.

- Feature: Laufzeit-Überwachung

Diese Erkenntnis informiert Sie darüber, dass ein Befehl ausgeführt wurde, mit dem versucht wird, einen Angriff vor den Sicherheitsdiensten des lokalen Systems zu verbergen. Dazu gehören Aktionen wie das Deaktivieren der Unix-Firewall, das Ändern lokaler IP-Tabellen, das Entfernen von crontab-Einträgen, das Deaktivieren eines lokalen Dienstes oder das Übernehmen der `LDPreload`-Funktion. Jede Änderung ist äußerst verdächtig und ein potenzieller Indikator für eine Gefährdung. Daher erkennen oder verhindern diese Mechanismen eine weitere Beeinträchtigung des Systems.

GuardDuty untersucht die zugehörige Laufzeitaktivität und den zugehörigen Kontext, sodass dieses Ergebnis nur generiert wird, wenn die zugehörige Aktivität und der Kontext potenziell verdächtig sind.

Der GuardDuty Runtime Agent überwacht Ereignisse von mehreren Ressourcen aus. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie sich den Ressourcentyp in den Ergebnisdetails in der GuardDuty Konsole an. Falls zutreffend, ist im Ergebnis zusätzlicher Kontext, einschließlich Informationen zum Prozess und zur Prozessherkunft, für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

DefenseEvasion:Runtime/PtraceAntiDebugging

Ein Prozess in einem Container oder auf einer Amazon-EC2-Instance hat mithilfe des ptrace-Systemaufrufs eine Anti-Debugging-Maßnahme ausgeführt.

Standard-Schweregrad: Niedrig

- Feature: Laufzeit-Überwachung

Dieses Ergebnis zeigt, dass ein Prozess, der auf der aufgeführten Amazon EC2-Instance oder einem Container in Ihrer AWS Umgebung ausgeführt wird, den ptrace-Systemaufruf mit der Option verwendet hat. `PTRACE_TRACEME` Diese Aktivität würde dazu führen, dass sich ein angefügter Debugger vom laufenden Prozess löst. Wenn kein Debugger angefügt ist, hat sie keine Wirkung. Die Aktivität an sich erregt jedoch Verdacht. Dies könnte darauf hindeuten, dass Malware auf dem System ausgeführt wird. Bei Malware werden häufig Anti-Debugging-Techniken verwendet, um der Analyse zu entgehen. Diese Techniken können zur Laufzeit erkannt werden.

GuardDuty untersucht die zugehörige Laufzeitaktivität und den zugehörigen Kontext, sodass dieses Ergebnis nur generiert wird, wenn die zugehörige Aktivität und der Kontext potenziell verdächtig sind.

Der GuardDuty Runtime Agent überwacht Ereignisse von mehreren Ressourcen aus. Um die betroffene Ressource zu identifizieren, sehen Sie in den Ergebnisdetails in der GuardDuty Konsole den Ressourcentyp an. Zusätzliche Informationen zum Kontext, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

Execution:Runtime/MaliciousFileExecuted

Eine bekannte bösartige ausführbare Datei wurde auf einer Amazon-EC2-Instance oder in einem Container ausgeführt.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass eine bekannte bösartige ausführbare Datei auf einer Amazon EC2-Instance oder einem Container in Ihrer AWS Umgebung ausgeführt wurde. Dies ist ein starker Indikator dafür, dass die Instance oder der Container potenziell kompromittiert und Malware ausgeführt wurde.

GuardDuty untersucht die zugehörige Laufzeitaktivität und den zugehörigen Kontext, sodass dieses Ergebnis nur generiert wird, wenn die zugehörige Aktivität und der Kontext potenziell verdächtig sind.

Der GuardDuty Runtime Agent überwacht Ereignisse von mehreren Ressourcen aus. Um die betroffene Ressource zu identifizieren, sehen Sie in den Ergebnisdetails in der GuardDuty Konsole den Ressourcentyp an. Falls zutreffend, ist im Ergebnis zusätzlicher Kontext, einschließlich Informationen zum Prozess und zur Prozessherkunft, für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

Execution:Runtime/MaliciousFileExecuted.Custom

Eine bösartige ausführbare Datei auf einer benutzerdefinierten Bedrohungsliste wurde auf einer Amazon-EC2-Instance oder in einem Container ausgeführt.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass eine ausführbare Datei, die in einer Bedrohungsliste enthalten ist, die Sie hochgeladen und aktiviert haben, auf einer Amazon EC2-Instance oder einem Container in Ihrer AWS Umgebung ausgeführt wurde. In GuardDuty: Eine Liste der Bedrohungsentitäten kann bekannte bösartige IP-Adressen, Domänen und SHA-256 Datei-Hashes enthalten. GuardDuty generiert Ergebnisse auf der Grundlage der Aktivität, die mit der hochgeladenen Liste der Bedrohungsentitäten verknüpft ist. Sie können den Namen der Bedrohungsentitätenliste in den Erkenntnisdetails einsehen.

Hinweis: Diese Erkenntnis wird nur ausgelöst, wenn eine ausführbare Datei ausgeführt wird, deren Hash in der Bedrohungsentitätenliste enthalten war.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcen. Um die betroffene Ressource zu identifizieren, sehen Sie in den Ergebnisdetails in der GuardDuty Konsole den Ressourcentyp an. Falls zutreffend, ist im Ergebnis zusätzlicher Kontext, einschließlich Informationen zum Prozess und zur Prozessherkunft, für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

Execution:Runtime/SuspiciousShellCreated

Ein Netzwerkdienst oder ein Prozess, auf den über das Netzwerk zugegriffen werden kann, auf einer Amazon EC2-Instance oder in einem Container hat einen interaktiven Shell-Prozess gestartet.

Standard-Schweregrad: Niedrig

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein über das Netzwerk zugänglicher Service auf einer Amazon EC2-Instance oder in einem Container in Ihrer AWS Umgebung eine interaktive Shell gestartet hat. Unter bestimmten Umständen kann dieses Szenario auf ein Verhalten nach der Ausnutzung hinweisen. Interaktive Shells ermöglichen es Angreifern, beliebige Befehle auf einer kompromittierten Instance oder einem kompromittierten Container auszuführen.

Der GuardDuty Runtime Agent überwacht Ereignisse von mehreren Ressourcen aus. Um die betroffene Ressource zu identifizieren, sehen Sie in den Ergebnisdetails in der GuardDuty Konsole den Ressourcentyp an. Zusätzliche Informationen zum Kontext, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar. Sie können die über das Netzwerk zugänglichen Prozessinformationen in den Details des übergeordneten Prozesses einsehen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

PrivilegeEscalation:Runtime/ElevationToRoot

Ein Prozess, der auf der aufgeführten Amazon EC2-Instance oder dem aufgelisteten Amazon EC2-Container ausgeführt wird, hat Root-Rechte übernommen.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein Prozess, der auf dem aufgeführten Amazon EC2 oder in dem aufgeführten Container in Ihrer AWS Umgebung ausgeführt wird, durch eine

ungewöhnliche oder verdächtige `setuid` Binärausführung Root-Rechte übernommen hat. Dies weist darauf hin, dass ein laufender Prozess potenziell kompromittiert wurde, und zwar für die EC2-Instance durch einen Exploit oder durch einen Exploit. `setuid` Mithilfe der Root-Rechte kann der Angreifer potenziell Befehle auf der Instance oder dem Container ausführen.

Es GuardDuty ist zwar so konzipiert, dass dieser Ergebnistyp nicht für Aktivitäten generiert wird, bei denen der `sudo` Befehl regelmäßig verwendet wird, aber es generiert dieses Ergebnis, wenn es die Aktivität als ungewöhnlich oder verdächtig einstuft.

GuardDuty untersucht die zugehörige Laufzeitaktivität und den Kontext und generiert diesen Ergebnistyp nur, wenn die zugehörige Aktivität und der Kontext ungewöhnlich oder verdächtig sind.

Der GuardDuty Runtime Agent überwacht Ereignisse von mehreren Ressourcen aus. Um die betroffene Ressource zu identifizieren, sehen Sie in den Ergebnisdetails in der GuardDuty Konsole den Ressourcentyp an. Zusätzliche Informationen zum Kontext, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

Discovery:Runtime/SuspiciousCommand

Ein verdächtiger Befehl wurde auf einer Amazon EC2-Instance oder in einem Container ausgeführt, der es einem Angreifer ermöglicht, Informationen über das lokale System und die Umgebung zu erhalten AWS Infrastruktur oder Container-Infrastruktur.

Standard-Schweregrad: Niedrig

Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein Prozess, der auf der aufgeführten Amazon EC2-Instance oder dem aufgelisteten Amazon EC2-Container in Ihrer AWS Umgebung ausgeführt wird, einen Befehl ausgeführt hat, der einem Angreifer wichtige Informationen liefern könnte, um den Angriff möglicherweise voranzutreiben. Die folgenden Informationen wurden möglicherweise abgerufen:

- Lokales System, wie etwa die Benutzer- oder Netzwerkkonfiguration,
- Andere verfügbare AWS Ressourcen und Berechtigungen oder
- Kubernetes-Infrastruktur wie Services und Pods.

Die Amazon EC2-Instance oder der Container, der in den Funddetails aufgeführt ist, wurde möglicherweise kompromittiert.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie sich den Ressourcentyp in den Ergebnisdetails in der GuardDuty Konsole an. Die Details zum verdächtigen Befehl finden Sie im `service.runtimeDetails.context`-Feld der JSON-Erkenntnisdatei. Zusätzliche Kontextinformationen, einschließlich Informationen zum Prozess und zur Prozessherkunft, sind im Ergebnis für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

Persistence:Runtime/SuspiciousCommand

Ein verdächtiger Befehl wurde auf einer Amazon EC2-Instance oder in einem Container ausgeführt, sodass ein Angreifer den Zugriff und die Kontrolle in Ihrem System aufrechterhalten kann AWS Umgebung.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein Prozess, der auf der aufgeführten Amazon EC2-Instance oder in einem Container in Ihrer AWS Umgebung ausgeführt wird, einen verdächtigen Befehl ausgeführt hat. Der Befehl installiert eine Persistenzmethode, mit der Malware ununterbrochen ausgeführt werden kann oder es einem Angreifer ermöglicht, kontinuierlich auf die potenziell gefährdete Instance oder den Container-Ressourcentyp zuzugreifen. Dies könnte möglicherweise bedeuten, dass ein Systemdienst installiert oder geändert wurde, geändert `crontab` wurde oder ein neuer Benutzer zur Systemkonfiguration hinzugefügt wurde.

GuardDuty untersucht die zugehörige Laufzeitaktivität und den zugehörigen Kontext und generiert diesen Ergebnistyp nur, wenn die zugehörige Aktivität und der Kontext ungewöhnlich oder verdächtig sind.

Die Amazon EC2-Instance oder der Container, der in den Ermittlungsdetails aufgeführt ist, wurde möglicherweise kompromittiert.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie sich den Ressourcentyp in den Ergebnisdetails in der GuardDuty Konsole an. Die Details zum verdächtigen Befehl finden Sie im `service.runtimeDetails.context`-Feld der JSON-Erkenntnisdatei. Falls zutreffend, ist im Ergebnis zusätzlicher Kontext, einschließlich Informationen zum Prozess und zur Prozessherkunft, für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

PrivilegeEscalation:Runtime/SuspiciousCommand

Ein verdächtiger Befehl wurde auf einer Amazon EC2-Instance oder in einem Container ausgeführt, wodurch ein Angreifer seine Rechte erweitern kann.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein Prozess, der auf der aufgeführten Amazon EC2-Instance oder in einem Container in Ihrer AWS Umgebung ausgeführt wird, einen verdächtigen Befehl ausgeführt hat. Der Befehl versucht, eine Rechteerweiterung durchzuführen, was es einem Gegner ermöglicht, Aufgaben mit hohen Rechten auszuführen.

GuardDuty untersucht die zugehörige Laufzeitaktivität und den zugehörigen Kontext und generiert diesen Ergebnistyp nur, wenn die zugehörige Aktivität und der Kontext ungewöhnlich oder verdächtig sind.

Die Amazon EC2-Instance oder der Container, der in den Ermittlungsdetails aufgeführt ist, wurde möglicherweise kompromittiert.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcen. Um die betroffene Ressource zu identifizieren, sehen Sie in den Ergebnisdetails in der GuardDuty Konsole den Ressourcentyp an. Falls zutreffend, ist im Ergebnis zusätzlicher Kontext, einschließlich Informationen zum Prozess und zur Prozessherkunft, für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

DefenseEvasion:Runtime/KernelModuleLoaded

Ein Kernelmodul wurde auf eine Amazon EC2-Instance geladen, was auf einen Versuch hindeutet, Zugriff auf Kernelebene zu erhalten.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Diese Erkenntnis weist darauf hin, dass ein Kernelmodul auf die aufgelistete EC2-Instance geladen wurde. Da Kernelmodule über die höchsten Berechtigungen auf Systemebene (Ring 0) verfügen, könnte dies darauf hindeuten, dass sich ein Bedrohungsakteur Zugriff auf Kernelebene verschafft hat. Diese Zugriffsebene ermöglicht die vollständige Kontrolle über das System.

Der GuardDuty Runtime Agent überwacht Ereignisse von mehreren Ressourcen aus. Um die betroffene Ressource zu identifizieren, sehen Sie in den Ergebnisdetails in der GuardDuty Konsole den Ressourcentyp an. Falls zutreffend, ist im Ergebnis zusätzlicher Kontext, einschließlich Informationen zum Prozess und zur Prozessherkunft, für weitere Untersuchungen verfügbar.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

Persistence:Runtime/SensitiveFileModified

Diese Erkenntnis informiert Sie darüber, dass ein verdächtiger Befehl auf einer Amazon-EC2-Instance oder in einer Amazon-EC2-Instance oder in einem Container ausgeführt wurde.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Diese Erkenntnis weist darauf hin, dass eine sicherheitsrelevante Systemdatei auf einer Amazon EC2-Instance oder in einem Container verändert wurde, wodurch ein Angreifer möglicherweise dauerhafte Ausführungsrechte auf dem System erlangen könnte. Dies könnte die Installation neuer SSH-Schlüsseldateien, Änderungen an Benutzerkonfigurationsdateien, Änderungen an Passwort- oder Shadow-Dateien, die Erstellung von geplanten Aufgaben, die Manipulation von Systemstartskripten oder die Änderung von ausführbaren Dateien oder Skriptdateien durch Webdienstprozesse in verdächtigen Kontexten umfassen. Diese Änderungen sind Anzeichen für eine Kompromittierung, die eine unbefugte Persistenz in Ihrer Umgebung ermöglichen könnten.

GuardDuty überwacht sicherheitsrelevante Systemdateien, die häufig von Gegnern angegriffen werden, um deren Persistenz zu gewährleisten. Da diese Dateien auch während der legitimen Systemadministration und -verwaltung geändert werden können, werden die zugehörigen Laufzeitaktivitäten und der Kontext GuardDuty untersucht, um diese Ergebnisse nur dann zu generieren, wenn Änderungen mit anderen verdächtigen Aktivitäten korrelieren.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie in der GuardDuty Konsole im Ergebnisbereich unter Ressourcentyp nach. Das Feld `service.runtimeDetails.context` enthält Details zur verdächtigen Dateiänderung, darunter den Dateipfad und die Art der Operation.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

PrivilegeEscalation:Runtime/SensitiveFileModified

Eine sicherheitsrelevante Systemdatei wurde auf einer Amazon EC2-Instance oder in einem Container verändert, wodurch ein Angreifer möglicherweise in die Lage versetzt wird, seine Berechtigungen zu erweitern.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Diese Erkenntnis weist darauf hin, dass eine sicherheitsrelevante Systemdatei auf einer Amazon EC2-Instance oder in einem Container verändert wurde, wodurch ein Angreifer möglicherweise in die Lage versetzt wird, seine Berechtigungen auf dem System zu erweitern. Dies könnte Änderungen an sicherheitskritischen Dateien wie der sudoers-Konfiguration, den PAM-Einstellungen oder den Systemauthentifizierungsdateien beinhalten. Diese Änderungen sind Anzeichen für eine Kompromittierung, die eine unbefugte Ausweitung von Berechtigungen ermöglichen könnten, was möglicherweise zu unbefugtem Root-Zugriff, geschwächten Authentifizierungsmechanismen oder beeinträchtigten Sicherheitskontrollen führen könnte.

GuardDuty überwacht sicherheitsrelevante Systemdateien, die häufig von Gegnern zur Rechteerweiterung ins Visier genommen werden. Da diese Dateien auch während der legitimen Systemadministration und -verwaltung geändert werden können, werden die zugehörigen Laufzeitaktivitäten und der Kontext GuardDuty untersucht, um diese Ergebnisse nur dann zu generieren, wenn Änderungen mit anderen verdächtigen Aktivitäten korrelieren.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie in der GuardDuty Konsole im Ergebnisbereich unter Ressourcentyp nach. Das Feld `service.runtimeDetails.context` enthält Details zur verdächtigen Dateiänderung, darunter den Dateipfad und die Art der Operation.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

DefenseEvasion:Runtime/SensitiveFileModified

Eine sicherheitsrelevante Systemdatei wurde auf einer Amazon EC2-Instance oder in einem Container verändert, wodurch ein Angreifer möglicherweise die Erkennung umgehen könnte.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Diese Erkenntnis weist darauf hin, dass eine sicherheitsrelevante Systemdatei auf einer Amazon EC2-Instance oder in einem Container verändert wurde, wodurch ein Angreifer möglicherweise die Erkennung durch das System umgehen könnte. Dies könnte Änderungen an Systemprotokolldateien, Audit-Konfigurationen, Befehlsverlaufsdateien oder Systemprotokollen umfassen. Diese Änderungen sind Anzeichen für eine Kompromittierung, die die Verschleierung unbefugter Aktivitäten, die Störung der Sicherheitsüberwachung oder die Beseitigung von Beweisen für Systemaktivitäten ermöglichen könnten.

GuardDuty überwacht sicherheitsrelevante Systemdateien, die häufig von Gegnern angegriffen werden, um die Verteidigung zu umgehen. Da diese Dateien auch während der legitimen Systemadministration und -verwaltung geändert werden können, werden die zugehörigen Laufzeitaktivitäten und der Kontext GuardDuty untersucht, um diese Ergebnisse nur dann zu generieren, wenn Änderungen mit anderen verdächtigen Aktivitäten korrelieren.

Der GuardDuty Runtime Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie in der GuardDuty Konsole im Ergebnisbereich unter Ressourcentyp nach. Das Feld `service.runtimeDetails.context` enthält Details zur verdächtigen Dateiänderung, darunter den Dateipfad und die Art der Operation.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Korrigieren von Erkenntnissen der Laufzeitüberwachung.

Malware-Schutz für EC2-Suchtypen

GuardDuty Malware Protection for EC2 bietet eine einzige Suche nach Malware Protection for EC2 für alle Bedrohungen, die beim Scan einer EC2-Instance oder eines Container-Workloads

erkannt wurden. Die Erkenntnis umfasst die Gesamtzahl der während des Scans entdeckten Bedrohungen und liefert, basierend auf dem Schweregrad, Details zu den 32 am häufigsten erkannten Bedrohungen. Im Gegensatz zu anderen GuardDuty Ergebnissen werden die Ergebnisse von Malware Protection for EC2 nicht aktualisiert, wenn dieselbe EC2-Instance oder dieselbe Container-Workload erneut gescannt wird.

Für jeden Scan, bei dem Malware erkannt wird, wird ein neues Ergebnis von Malware Protection for EC2 generiert. Die Ergebnisse von Malware Protection for EC2 umfassen Informationen über den entsprechenden Scan, der zu dem Ergebnis geführt hat, sowie über das GuardDuty Ergebnis, das diesen Scan ausgelöst hat. Dadurch ist es einfacher, das verdächtige Verhalten mit der erkannten Malware zu korrelieren.

> **Note**
>
> Wenn bösartige Aktivitäten auf einem Container-Workload GuardDuty erkannt werden, generiert Malware Protection for EC2 kein Ergebnis auf EC2-Ebene.

Die folgenden Ergebnisse beziehen sich speziell auf GuardDuty Malware Protection for EC2.

Themen

- Execution:EC2/MaliciousFile
- Execution:ECS/MaliciousFile
- Execution:Kubernetes/MaliciousFile
- Execution:Container/MaliciousFile
- Execution:EC2/SuspiciousFile
- Execution:ECS/SuspiciousFile
- Execution:Kubernetes/SuspiciousFile
- Execution:Container/SuspiciousFile

Execution:EC2/MaliciousFile

Auf einer EC2-Instance wurde eine schädliche Datei entdeckt.

Standardschweregrad: Variiert je nach erkannter Bedrohung.

- Merkmal: EBS-Malware-Schutz

Dieses Ergebnis weist darauf hin, dass der Scan von GuardDuty Malware Protection for EC2 eine oder mehrere schädliche Dateien auf der aufgelisteten EC2-Instance in Ihrer Umgebung entdeckt hat. AWS Die aufgeführte Instance ist möglicherweise kompromittiert. Weitere Informationen finden Sie im Abschnitt Entdeckte Bedrohungen in den Details zu den Erkenntnissen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Execution:ECS/MaliciousFile

Auf einem ECS-Cluster wurde eine bösartige Datei entdeckt.

Standardschweregrad: Variiert je nach erkannter Bedrohung.

- Funktion: EBS-Malware-Schutz

Dieses Ergebnis weist darauf hin, dass der Scan von GuardDuty Malware Protection for EC2 eine oder mehrere schädliche Dateien auf einem Container-Workload entdeckt hat, der zu einem ECS-Cluster gehört. Weitere Informationen finden Sie im Abschnitt Entdeckte Bedrohungen in den Details zu den Erkenntnissen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität unerwartet ist, ist Ihr Container, der zum ECS-Cluster gehört, möglicherweise kompromittiert. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten ECS-Clusters.

Execution:Kubernetes/MaliciousFile

Auf einem Kubernetes-Cluster wurde eine bösartige Datei entdeckt.

Standardschweregrad: Variiert je nach erkannter Bedrohung.

- Funktion: EBS-Malware-Schutz

Dieses Ergebnis weist darauf hin, dass der Scan von GuardDuty Malware Protection for EC2 eine oder mehrere schädliche Dateien auf einem Container-Workload entdeckt hat, der zu einem Kubernetes-Cluster gehört. Wenn es sich um einen von EKS verwalteten Cluster handelt, enthalten

die Erkenntnisdetails zusätzliche Informationen über die betroffene EKS-Ressource. Weitere Informationen finden Sie im Abschnitt Entdeckte Bedrohungen in den Details zu den Erkenntnissen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität unerwartet ist, kann Ihr Container-Workload kompromittiert sein. Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

Execution:Container/MaliciousFile

In einem eigenständigen Container wurde eine bösartige Datei entdeckt.

Standardschweregrad: Variiert je nach erkannter Bedrohung.

- Funktion: EBS-Malware-Schutz

Dieses Ergebnis weist darauf hin, dass der Scan von GuardDuty Malware Protection for EC2 eine oder mehrere schädliche Dateien auf einem Container-Workload erkannt hat und keine Clusterinformationen identifiziert wurden. Weitere Informationen finden Sie im Abschnitt Entdeckte Bedrohungen in den Details zu den Erkenntnissen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität unerwartet ist, kann Ihr Container-Workload kompromittiert sein. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten Standalone-Containers.

Execution:EC2/SuspiciousFile

Auf einer EC2-Instance wurde eine verdächtige Datei entdeckt.

Standardschweregrad: Variiert je nach erkannter Bedrohung.

- Funktion: EBS-Malware-Schutz

Dieses Ergebnis weist darauf hin, dass der Scan von GuardDuty Malware Protection for EC2 eine oder mehrere verdächtige Dateien auf einer EC2-Instance erkannt hat. Weitere Informationen finden Sie im Abschnitt Entdeckte Bedrohungen in den Details zu den Erkenntnissen.

Erkenntnisse vom Typ `SuspiciousFile` deuten darauf hin, dass sich auf einer betroffenen Ressource potenziell unerwünschte Programme wie Adware, Spyware oder Tools mit doppeltem

Verwendungszweck befinden. Diese Programme können sich negativ auf Ihre Ressource auswirken oder von Angreifern für böswillige Zwecke verwendet werden. Netzwerktools können beispielsweise von Gegnern legitim oder böswillig als Hacking-Tools verwendet werden, um zu versuchen, Ressourcen zu kompromittieren.

Wenn eine verdächtige Datei erkannt wurde, prüfen Sie, ob Sie davon ausgehen, dass die erkannte Datei in Ihrer AWS Umgebung angezeigt wird. Falls die Datei unerwartet ist, befolgen Sie die Empfehlungen zur Problembehebung im nächsten Abschnitt.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Execution:ECS/SuspiciousFile

Auf einem ECS-Cluster wurde eine verdächtige Datei entdeckt.

Standardschweregrad: Variiert je nach erkannter Bedrohung.

- Funktion: EBS-Malware-Schutz

Dieses Ergebnis weist darauf hin, dass der Scan von GuardDuty Malware Protection for EC2 eine oder mehrere verdächtige Dateien in einem Container entdeckt hat, der zu einem ECS-Cluster gehört. Weitere Informationen finden Sie im Abschnitt Entdeckte Bedrohungen in den Details zu den Erkenntnissen.

Erkenntnisse vom Typ `SuspiciousFile` deuten darauf hin, dass sich auf einer betroffenen Ressource potenziell unerwünschte Programme wie Adware, Spyware oder Tools mit doppeltem Verwendungszweck befinden. Diese Programme können sich negativ auf Ihre Ressource auswirken oder von Angreifern für böswillige Zwecke verwendet werden. Netzwerktools können beispielsweise von Gegnern legitim oder böswillig als Hacking-Tools verwendet werden, um zu versuchen, Ressourcen zu kompromittieren.

Wenn eine verdächtige Datei erkannt wurde, prüfen Sie, ob Sie damit rechnen, die erkannte Datei in Ihrer AWS Umgebung zu sehen. Falls die Datei unerwartet ist, befolgen Sie die Empfehlungen zur Problembehebung im nächsten Abschnitt.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität unerwartet ist, ist Ihr Container, der zum ECS-Cluster gehört, möglicherweise kompromittiert. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten ECS-Clusters.

Execution:Kubernetes/SuspiciousFile

In einem Kubernetes-Cluster wurde eine verdächtige Datei entdeckt.

Standardschweregrad: Variiert je nach erkannter Bedrohung.

- Funktion: EBS-Malware-Schutz

Dieses Ergebnis weist darauf hin, dass der Scan von GuardDuty Malware Protection for EC2 eine oder mehrere verdächtige Dateien in einem Container erkannt hat, der zu einem Kubernetes-Cluster gehört. Wenn es sich um einen von EKS verwalteten Cluster handelt, enthalten die Erkenntnisdetails zusätzliche Informationen über die betroffene EKS-Ressource. Weitere Informationen finden Sie im Abschnitt Entdeckte Bedrohungen in den Details zu den Erkenntnissen.

Erkenntnisse vom Typ `SuspiciousFile` deuten darauf hin, dass sich auf einer betroffenen Ressource potenziell unerwünschte Programme wie Adware, Spyware oder Tools mit doppeltem Verwendungszweck befinden. Diese Programme können sich negativ auf Ihre Ressource auswirken oder von Angreifern für böswillige Zwecke verwendet werden. Netzwerktools können beispielsweise von Gegnern legitim oder böswillig als Hacking-Tools verwendet werden, um zu versuchen, Ressourcen zu kompromittieren.

Wenn eine verdächtige Datei erkannt wurde, prüfen Sie, ob Sie damit rechnen, die erkannte Datei in Ihrer Umgebung zu sehen. AWS Falls die Datei unerwartet ist, befolgen Sie die Empfehlungen zur Problembehebung im nächsten Abschnitt.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität unerwartet ist, kann Ihr Container-Workload kompromittiert sein. Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

Execution:Container/SuspiciousFile

In einem eigenständigen Container wurde eine verdächtige Datei entdeckt.

Standardschweregrad: Variiert je nach erkannter Bedrohung.

- Funktion: EBS-Malware-Schutz

Dieses Ergebnis weist darauf hin, dass der Scan von GuardDuty Malware Protection for EC2 eine oder mehrere verdächtige Dateien in einem Container ohne Clusterinformationen erkannt hat. Weitere Informationen finden Sie im Abschnitt Entdeckte Bedrohungen in den Details zu den Erkenntnissen.

Erkenntnisse vom Typ `SuspiciousFile` deuten darauf hin, dass sich auf einer betroffenen Ressource potenziell unerwünschte Programme wie Adware, Spyware oder Tools mit doppeltem Verwendungszweck befinden. Diese Programme können sich negativ auf Ihre Ressource auswirken oder von Angreifern für böswillige Zwecke verwendet werden. Netzwerktools können beispielsweise von Gegnern legitim oder böswillig als Hacking-Tools verwendet werden, um zu versuchen, Ressourcen zu kompromittieren.

Wenn eine verdächtige Datei erkannt wurde, prüfen Sie, ob Sie damit rechnen, die entdeckte Datei in Ihrer AWS Umgebung zu sehen. Falls die Datei unerwartet ist, befolgen Sie die Empfehlungen zur Problembehebung im nächsten Abschnitt.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität unerwartet ist, kann Ihr Container-Workload kompromittiert sein. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten Standalone-Containers.

Suchtyp „Malware-Schutz für S3“

GuardDuty generiert nur dann einen Befund, wenn eine potenzielle Sicherheitsbedrohung in Ihrem erkannt wird AWS-Konto. Ein Ergebnis von Malware Protection for S3 weist darauf hin, dass das hochgeladene Objekt, das den Malware-Scan initiiert hat, eine potenziell schädliche Datei enthält.

GuardDuty Damit Amazon ein Ergebnis in Ihrem generiert AWS-Konto, aktivieren Sie GuardDuty sowohl als auch Malware Protection for S3. Es hat sich bewährt, zuerst den Malware-Schutz für S3 zu aktivieren GuardDuty und dann. Wenn diese Reihenfolge für Sie anders ist, stellen Sie sicher, dass Sie sie aktivieren, GuardDuty bevor ein S3-Objekt in Ihren geschützten Bucket hochgeladen wird.

> **Note**
>
> GuardDuty kann keinen Befund für ein S3-Objekt generieren, das vor der Aktivierung gescannt wurde GuardDuty. Um ein vorhandenes S3-Objekt zu scannen, können Sie es erneut hochladen.

Object:S3/MaliciousFile

Auf einem gescannten S3-Objekt wurde eine schädliche Datei entdeckt.

Standard-Schweregrad: Hoch

- Funktion: Malware-Schutz für S3

Diese Erkenntnis weist darauf hin, dass ein Malware-Scan das aufgelistete S3-Objekt als schädlich erkannt hat. Weitere Informationen finden Sie im Abschnitt Entdeckte Bedrohungen im Bereich mit den Funddetails.

Empfehlung zur Behebung:

Wenn diese Erkenntnis unerwartet war, ist das S3-Objekt potenziell schädlich. Informationen zu empfohlenen Behebungsschritten finden Sie unter. Behebung eines potenziell bösartigen S3-Objekts

Malware-Schutz für Backup-Suchtypen

GuardDuty Malware Protection for Backup bietet eine einzige Suche für alle Bedrohungen, die beim Scannen der angeforderten Ressource erkannt wurden. Die Erkenntnis umfasst die Gesamtzahl der während des Scans entdeckten Bedrohungen und liefert, basierend auf dem Schweregrad, Details zu den 32 am häufigsten erkannten Bedrohungen. Im Gegensatz zu anderen GuardDuty Ergebnissen werden die Ergebnisse von Malware Protection for Backup nicht aktualisiert, wenn dieselbe Ressource erneut gescannt wird. Für jeden Scan, der Malware entdeckt, wird eine neue Entdeckung von Malware Protection for Backup generiert.

Die folgenden Ergebnisse beziehen sich speziell auf GuardDuty Malware Protection for Backup.

Themen

- Execution:EC2/MaliciousFile!Snapshot

- Execution:EC2/MaliciousFile!AMI
- Execution:EC2/MaliciousFile!RecoveryPoint
- Execution:S3/MaliciousFile!RecoveryPoint

Execution:EC2/MaliciousFile!Snapshot

In einem EBS-Snapshot wurde eine schädliche Datei entdeckt.

Standardschweregrad: Variiert je nach erkannter Bedrohung.

- Feature: Malware-Schutz für Backup

Dieses Ergebnis weist darauf hin, dass ein Scan von GuardDuty Malware Protection for Backup eine oder mehrere schädliche Dateien in einem EBS-Snapshot in Ihrer Umgebung entdeckt hat. Weitere Informationen finden Sie im Abschnitt „Erkannte Bedrohungen“ im Detailfenster „Erkenntnisse“.

Empfehlungen zur Abhilfe:

Wenn dies nicht erwartet wird, ist Ihr Snapshot möglicherweise kompromittiert. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten EBS-Snapshots.

Execution:EC2/MaliciousFile!AMI

In einem EC2-AMI wurde eine schädliche Datei entdeckt.

Standardschweregrad: Variiert je nach erkannter Bedrohung.

- Feature: Malware-Schutz für Backup

Dieses Ergebnis deutet darauf hin, dass ein Scan von GuardDuty Malware Protection for Backup eine oder mehrere schädliche Dateien in einem AMI in Ihrer Umgebung entdeckt hat. Weitere Informationen finden Sie im Abschnitt „Erkannte Bedrohungen“ im Detailfenster „Erkenntnisse“.

Empfehlungen zur Abhilfe:

Wenn dies nicht erwartet wird, ist Ihr AMI möglicherweise kompromittiert. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten EC2-AMI.

Execution:EC2/MaliciousFile!RecoveryPoint

In einem AWS Backup EC2 Recovery Point wurde eine schädliche Datei entdeckt.

Standardschweregrad: Variiert je nach erkannter Bedrohung.

- Feature: Malware-Schutz für Backup

Dieses Ergebnis deutet darauf hin, dass ein Scan von GuardDuty Malware Protection for Backup eine oder mehrere schädliche Dateien in einem EC2-Wiederherstellungspunkt in Ihrer Umgebung entdeckt hat. Der betroffene Wiederherstellungspunkt Point könnte ein EBS-Snapshot oder ein EC2-AMI sein. Weitere Informationen finden Sie im Abschnitt „Erkannte Bedrohungen“ im Detailfenster „Erkenntnisse“.

Empfehlungen zur Abhilfe:

Wenn dies nicht erwartet wird, ist Ihr EC2-Wiederherstellungspunkt möglicherweise kompromittiert. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten EC2-Wiederherstellungspunkts.

Execution:S3/MaliciousFile!RecoveryPoint

In einem AWS Backup S3 Recovery Point wurde eine schädliche Datei entdeckt.

Standardschweregrad: Variiert je nach erkannter Bedrohung.

- Feature: Malware-Schutz für Backup

Dieses Ergebnis deutet darauf hin, dass ein Scan von GuardDuty Malware Protection for Backup ein oder mehrere schädliche Objekte in einem S3-Wiederherstellungspunkt in Ihrer Umgebung entdeckt hat. Weitere Informationen finden Sie im Abschnitt „Erkannte Bedrohungen“ im Detailfenster „Erkenntnisse“.

Empfehlungen zur Abhilfe:

Wenn dies nicht erwartet wird, ist Ihr S3-Wiederherstellungspunkt möglicherweise kompromittiert. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten S3-Wiederherstellungspunkts.

GuardDuty Suchtypen für den RDS-Schutz

GuardDuty RDS Protection erkennt ungewöhnliches Anmeldeverhalten auf Ihrer Datenbank-Instance. Die folgenden Ergebnisse beziehen sich auf den Unterstützte Amazon Aurora-, Amazon RDS- und Aurora Limitless-Datenbanken und haben einen Ressourcentyp von **`RDSDBInstance`** oder. `RDSLimitlessDB` Der Schweregrad und die Details der Ergebnisse unterscheiden sich je nach Erkennungstyp.

Themen

- CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin
- CredentialAccess:RDS/AnomalousBehavior.FailedLogin
- CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce
- CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin
- CredentialAccess:RDS/MaliciousIPCaller.FailedLogin
- Discovery:RDS/MaliciousIPCaller
- CredentialAccess:RDS/TorIPCaller.SuccessfulLogin
- CredentialAccess:RDS/TorIPCaller.FailedLogin
- Discovery:RDS/TorIPCaller

CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin

Ein Benutzer hat sich erfolgreich auf ungewöhnliche Weise bei einer RDS-Datenbank in Ihrem Konto angemeldet.

Standardschweregrad: Variabel

> **Note**
>
> Je nach dem anomalen Verhalten, das mit diesem Ergebnis einhergeht, kann der Standardschweregrad Niedrig, Mittel und Hoch gewählt werden.
>
> - Niedrig – Wenn der mit diesem Ergebnis verknüpfte Benutzername von einer IP-Adresse aus angemeldet ist, die einem privaten Netzwerk zugeordnet ist.
> - Mittel – Wenn der mit diesem Ergebnis verknüpfte Benutzername von einer öffentlichen IP-Adresse aus angemeldet ist.

- Hoch – Wenn es ein einheitliches Muster von fehlgeschlagenen Anmeldeversuchen von öffentlichen IP-Adressen aus gibt, was auf zu freizügige Zugriffsrichtlinien hindeutet.

- Feature: Überwachung der RDS-Anmeldeaktivitäten

Dieses Ergebnis informiert Sie darüber, dass eine ungewöhnliche erfolgreiche Anmeldung bei einer RDS-Datenbank in Ihrer AWS Umgebung beobachtet wurde. Dies kann darauf hindeuten, dass sich ein zuvor unbekannter Benutzer zum ersten Mal bei einer RDS-Datenbank angemeldet hat. Ein häufiges Szenario ist ein interner Benutzer, der sich bei einer Datenbank anmeldet, auf die programmgesteuert von Anwendungen und nicht von einzelnen Benutzern zugegriffen wird.

Diese erfolgreiche Anmeldung wurde anhand des ML-Modells (Machine Learning) zur Erkennung von GuardDuty Anomalien als ungewöhnlich eingestuft. Das ML-Modell bewertet alle Datenbank-Anmeldeereignisse in Ihrer Unterstützte Amazon Aurora-, Amazon RDS- und Aurora Limitless-Datenbanken und identifiziert anomale Ereignisse, die mit den von Gegnern verwendeten Techniken in Verbindung stehen. Das ML-Modell verfolgt verschiedene Faktoren der RDS-Anmeldeaktivität, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und die spezifischen Datenbank-Verbindungsdetails, die verwendet wurden. Informationen zu potenziell ungewöhnlichen Anmeldeereignissen finden Sie unter Anomalien aufgrund von RDS-Anmeldeaktivitäten.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für die zugehörige Datenbank unerwartet ist, wird empfohlen, das Passwort des zugehörigen Datenbankbenutzers zu ändern und die verfügbaren Audit-Logs auf Aktivitäten zu überprüfen, die von dem anomalen Benutzer ausgeführt wurden. Erkenntnisse mit mittlerem und hohem Schweregrad können darauf hindeuten, dass die Zugriffsrichtlinien für die Datenbank zu freizügig sind und die Anmeldeinformationen der Benutzer möglicherweise offengelegt oder kompromittiert wurden. Es wird empfohlen, die Datenbank in einer privaten VPC zu platzieren und die Sicherheitsgruppenregeln so zu beschränken, dass nur Datenverkehr aus den erforderlichen Quellen zugelassen wird. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Datenbank mit erfolgreichen Anmeldeereignissen.

CredentialAccess:RDS/AnomalousBehavior.FailedLogin

Ein oder mehrere ungewöhnliche fehlgeschlagene Anmeldeversuche wurden in einer RDS-Datenbank in Ihrem Konto beobachtet.

Standard-Schweregrad: Niedrig

- Feature: Überwachung der RDS-Anmeldeaktivitäten

Dieses Ergebnis informiert Sie darüber, dass eine oder mehrere anomale fehlgeschlagene Anmeldungen in einer RDS-Datenbank in Ihrer Umgebung beobachtet wurden. AWS Fehlgeschlagene Anmeldeversuche von öffentlichen IP-Adressen aus können darauf hindeuten, dass die RDS-Datenbank in Ihrem Konto einem Brute-Force-Angriff durch einen potenziell böswilligen Akteur ausgesetzt war.

Diese fehlgeschlagenen Anmeldungen wurden durch das ML-Modell (Machine Learning) zur Erkennung von GuardDuty Anomalien als anomal identifiziert. Das ML-Modell bewertet alle Datenbank-Anmeldeereignisse in Ihrer Unterstützte Amazon Aurora-, Amazon RDS- und Aurora Limitless-Datenbanken und identifiziert anomale Ereignisse, die mit den von Gegnern verwendeten Techniken in Verbindung stehen. Das ML-Modell verfolgt verschiedene Faktoren der RDS-Anmeldeaktivität, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und die spezifischen Datenbank-Verbindungsdetails, die verwendet wurden. Informationen zu potenziell ungewöhnlichen RDS-Anmeldeaktivitäten finden Sie unter Anomalien aufgrund von RDS-Anmeldeaktivitäten.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für die zugehörige Datenbank unerwartet ist, kann dies darauf hindeuten, dass die Datenbank öffentlich zugänglich ist oder dass es eine zu freizügige Zugriffsrichtlinie für die Datenbank gibt. Es wird empfohlen, die Datenbank in einer privaten VPC zu platzieren und die Sicherheitsgruppenregeln so zu beschränken, dass nur Datenverkehr aus den erforderlichen Quellen zugelassen wird. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Datenbank mit erfolglosen Anmeldeereignissen.

CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce

Ein Benutzer hat sich nach einem konsistenten Muster ungewöhnlicher fehlgeschlagener Anmeldeversuche erfolgreich von einer öffentlichen IP-Adresse aus auf ungewöhnliche Weise bei einer RDS-Datenbank in Ihrem Konto angemeldet.

Standard-Schweregrad: Hoch

- Feature: Überwachung der RDS-Anmeldeaktivitäten

Dieses Ergebnis informiert Sie darüber, dass bei einer RDS-Datenbank in Ihrer Umgebung eine anomale Anmeldung beobachtet wurde, die auf eine erfolgreiche Brute-Force-Operation hindeutet. AWS Vor einer anomalen erfolgreichen Anmeldung wurde ein konsistentes Muster ungewöhnlicher fehlgeschlagener Anmeldeversuche beobachtet. Dies deutet darauf hin, dass der Benutzer und das Passwort, die mit der RDS-Datenbank in Ihrem Konto verknüpft sind, möglicherweise kompromittiert wurden und dass möglicherweise ein potenziell böswilliger Akteur auf die RDS-Datenbank zugegriffen hat.

Diese erfolgreiche Brute-Force-Anmeldung wurde durch das ML-Modell (Machine Learning) zur Erkennung von GuardDuty Anomalien als anomal identifiziert. Das ML-Modell bewertet alle Datenbank-Anmeldeereignisse in Ihrer Unterstützte Amazon Aurora-, Amazon RDS- und Aurora Limitless-Datenbanken und identifiziert anomale Ereignisse, die mit den von Gegnern verwendeten Techniken in Verbindung stehen. Das ML-Modell verfolgt verschiedene Faktoren der RDS-Anmeldeaktivität, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und die spezifischen Datenbank-Verbindungsdetails, die verwendet wurden. Informationen zu potenziell ungewöhnlichen RDS-Anmeldeaktivitäten finden Sie unter Anomalien aufgrund von RDS-Anmeldeaktivitäten.

Empfehlungen zur Abhilfe:

Diese Aktivität weist darauf hin, dass Datenbankanmeldeinformationen möglicherweise offengelegt oder kompromittiert wurden. Es wird empfohlen, das Passwort des zugehörigen Datenbankbenutzers zu ändern und die verfügbaren Prüfungsprotokolle auf Aktivitäten des potenziell kompromittierten Benutzers zu überprüfen. Ein konsistentes Muster ungewöhnlicher fehlgeschlagener Anmeldeversuche deutet auf eine zu freizügige Zugriffsrichtlinie auf die Datenbank hin, oder die Datenbank wurde möglicherweise auch öffentlich zugänglich gemacht. Es wird empfohlen, die Datenbank in einer privaten VPC zu platzieren und die Sicherheitsgruppenregeln so zu beschränken,

dass nur Datenverkehr aus den erforderlichen Quellen zugelassen wird. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Datenbank mit erfolgreichen Anmeldeereignissen.

CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin

Ein Benutzer hat sich erfolgreich von einer bekannten bösartigen IP-Adresse aus bei einer RDS-Datenbank in Ihrem Konto angemeldet.

Standard-Schweregrad: Hoch

- Feature: Überwachung der RDS-Anmeldeaktivitäten

Dieses Ergebnis informiert Sie darüber, dass eine erfolgreiche RDS-Anmeldeaktivität von einer IP-Adresse aus erfolgte, die mit einer bekannten bösartigen Aktivität in Ihrer Umgebung in Verbindung steht. AWS Dies deutet darauf hin, dass der Benutzer und das Passwort, die mit der RDS-Datenbank in Ihrem Konto verknüpft sind, möglicherweise kompromittiert wurden und dass möglicherweise ein potenziell böswilliger Akteur auf die RDS-Datenbank zugegriffen hat.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für die zugehörige Datenbank unerwartet ist, kann dies darauf hindeuten, dass die Benutzeranmeldeinformationen möglicherweise offengelegt oder kompromittiert wurden. Es wird empfohlen, das Passwort des zugehörigen Datenbankbenutzers zu ändern und die verfügbaren Prüfungsprotokolle auf Aktivitäten des potenziell kompromittiert Benutzers zu überprüfen. Wenn diese Aktivität für die zugehörige Datenbank unerwartet ist, kann dies darauf hindeuten, dass die Datenbank öffentlich zugänglich ist oder dass es eine zu freizügige Zugriffsrichtlinie für die Datenbank gibt. Es wird empfohlen, die Datenbank in einer privaten VPC zu platzieren und die Sicherheitsgruppenregeln so zu beschränken, dass nur Datenverkehr aus den erforderlichen Quellen zugelassen wird. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Datenbank mit erfolgreichen Anmeldeereignissen.

CredentialAccess:RDS/MaliciousIPCaller.FailedLogin

Eine IP-Adresse, die mit einer bekannten böswilligen Aktivität verknüpft ist, hat erfolglos versucht, sich bei einer RDS-Datenbank in Ihrem Konto anzumelden.

Standard-Schweregrad: Mittel

- Feature: Überwachung der RDS-Anmeldeaktivitäten

Dieses Ergebnis informiert Sie darüber, dass eine IP-Adresse, die mit bekannten böswilligen Aktivitäten in Verbindung steht, versucht hat, sich bei einer RDS-Datenbank in Ihrer AWS Umgebung anzumelden, dabei aber nicht den richtigen Benutzernamen oder das richtige Passwort angegeben hat. Dies deutet darauf hin, dass ein potenziell böswilliger Akteur versucht, die RDS-Datenbank in Ihrem Konto zu kompromittieren.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für die zugehörige Datenbank unerwartet ist, kann dies darauf hindeuten, dass die Datenbank öffentlich zugänglich ist oder dass es eine zu freizügige Zugriffsrichtlinie für die Datenbank gibt. Es wird empfohlen, die Datenbank in einer privaten VPC zu platzieren und die Sicherheitsgruppenregeln so zu beschränken, dass nur Datenverkehr aus den erforderlichen Quellen zugelassen wird. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Datenbank mit erfolglosen Anmeldeereignissen.

Discovery:RDS/MaliciousIPCaller

Eine IP-Adresse, die mit einer bekannten böswilligen Aktivität in Verbindung steht, hat eine RDS-Datenbank in Ihrem Konto untersucht. Es wurde kein Authentifizierungsversuch unternommen.

Standard-Schweregrad: Mittel

- Feature: Überwachung der RDS-Anmeldeaktivitäten

Dieses Ergebnis informiert Sie darüber, dass eine IP-Adresse, die mit einer bekannten böswilligen Aktivität verknüpft ist, eine RDS-Datenbank in Ihrer AWS Umgebung untersucht hat, obwohl kein Anmeldeversuch unternommen wurde. Dies kann darauf hindeuten, dass ein potenziell böswilliger Akteur versucht, nach einer öffentlich zugänglichen Infrastruktur zu scannen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für die zugehörige Datenbank unerwartet ist, kann dies darauf hindeuten, dass die Datenbank öffentlich zugänglich ist oder dass es eine zu freizügige Zugriffsrichtlinie für die Datenbank gibt. Es wird empfohlen, die Datenbank in einer privaten VPC zu platzieren und die Sicherheitsgruppenregeln so zu beschränken, dass nur Datenverkehr aus den erforderlichen Quellen zugelassen wird. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Datenbank mit erfolglosen Anmeldeereignissen.

CredentialAccess:RDS/TorIPCaller.SuccessfulLogin

Ein Benutzer hat sich erfolgreich über eine IP-Adresse des Tor-Ausgangsknotens bei einer RDS-Datenbank in Ihrem Konto angemeldet.

Standard-Schweregrad: Hoch

- Feature: Überwachung der RDS-Anmeldeaktivitäten

Dieses Ergebnis informiert Sie darüber, dass sich ein Benutzer erfolgreich von einer IP-Adresse des Tor-Ausgangsknotens aus bei einer RDS-Datenbank in Ihrer AWS -Umgebung angemeldet hat. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese nach dem Zufallsprinzip durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Dies kann auf einen unbefugten Zugriff auf die RDS-Ressourcen hinweisen, der das Ziel hat, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für die zugehörige Datenbank unerwartet ist, kann dies darauf hindeuten, dass die Benutzeranmeldeinformationen möglicherweise offengelegt oder kompromittiert wurden. Es wird empfohlen, das Passwort des zugehörigen Datenbankbenutzers zu ändern und die verfügbaren Prüfungsprotokolle auf Aktivitäten des potenziell kompromittiert Benutzers zu überprüfen. Wenn diese Aktivität für die zugehörige Datenbank unerwartet ist, kann dies darauf hindeuten, dass die Datenbank öffentlich zugänglich ist oder dass es eine zu freizügige Zugriffsrichtlinie für die Datenbank gibt. Es wird empfohlen, die Datenbank in einer privaten VPC zu platzieren und die Sicherheitsgruppenregeln so zu beschränken, dass nur Datenverkehr aus den erforderlichen Quellen zugelassen wird. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Datenbank mit erfolgreichen Anmeldeereignissen.

CredentialAccess:RDS/TorIPCaller.FailedLogin

Eine Tor-IP-Adresse hat erfolglos versucht, sich bei einer RDS-Datenbank in Ihrem Konto anzumelden.

Standard-Schweregrad: Mittel

- Feature: Überwachung der RDS-Anmeldeaktivitäten

Dieses Ergebnis informiert Sie darüber, dass die IP-Adresse eines Tor-Ausgangsknotens versucht hat, sich bei einer RDS-Datenbank in Ihrer AWS Umgebung anzumelden, aber nicht den richtigen Benutzernamen oder das richtige Passwort angegeben hat. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese nach dem Zufallsprinzip durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Dies kann auf einen unbefugten Zugriff auf die RDS-Ressourcen hinweisen, der das Ziel hat, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für die zugehörige Datenbank unerwartet ist, kann dies darauf hindeuten, dass die Datenbank öffentlich zugänglich ist oder dass es eine zu freizügige Zugriffsrichtlinie für die Datenbank gibt. Es wird empfohlen, die Datenbank in einer privaten VPC zu platzieren und die Sicherheitsgruppenregeln so zu beschränken, dass nur Datenverkehr aus den erforderlichen Quellen zugelassen wird. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Datenbank mit erfolglosen Anmeldeereignissen.

Discovery:RDS/TorIPCaller

Eine IP-Adresse des Tor-Ausgangsknotens hat eine RDS-Datenbank in Ihrem Konto untersucht, es wurde kein Authentifizierungsversuch unternommen.

Standard-Schweregrad: Mittel

- Feature: Überwachung der RDS-Anmeldeaktivitäten

Diese Erkenntnis informiert Sie darüber, dass die IP-Adresse eines Tor-Ausgangsknotens eine RDS-Datenbank in Ihrer AWS -Umgebung untersucht hat, obwohl kein Anmeldeversuch unternommen wurde. Dies kann darauf hindeuten, dass ein potenziell böswilliger Akteur versucht, nach einer öffentlich zugänglichen Infrastruktur zu scannen. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese beliebig durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Dies kann auf einen unbefugten Zugriff auf die RDS-Ressourcen in Ihrem Konto hinweisen, der das Ziel hat, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für die zugehörige Datenbank unerwartet ist, kann dies darauf hindeuten, dass die Datenbank öffentlich zugänglich ist oder dass es eine zu freizügige Zugriffsrichtlinie für

die Datenbank gibt. Es wird empfohlen, die Datenbank in einer privaten VPC zu platzieren und die Sicherheitsgruppenregeln so zu beschränken, dass nur Datenverkehr aus den erforderlichen Quellen zugelassen wird. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Datenbank mit erfolglosen Anmeldeereignissen.

Lambda-Protection-Erkenntnistypen

In diesem Abschnitt werden die Findetypen beschrieben, die für Ihre AWS Lambda Ressourcen spezifisch sind und in denen sie als `resourceType` `Lambda` aufgeführt sind. Für alle Lambda-Erkenntnisse wird empfohlen, die betreffende Ressource zu untersuchen, um festzustellen, ob sie sich erwartungsgemäß verhält. Wenn die Aktivität autorisiert ist, können Sie Unterdrückungsregeln oder Listen vertrauenswürdiger IP-Adressen und Bedrohungen verwenden, um Falschmeldungen für diese Ressource zu verhindern.

Wenn die Aktivität unerwartet ist, besteht die bewährte Sicherheitsmethode darin, davon auszugehen, dass Lambda potenziell kompromittiert wurde, und die Empfehlungen zur Behebung zu befolgen.

Themen

- Backdoor:Lambda/C&CActivity.B
- CryptoCurrency:Lambda/BitcoinTool.B
- Trojan:Lambda/BlackholeTraffic
- Trojan:Lambda/DropPoint
- UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom
- UnauthorizedAccess:Lambda/TorClient
- UnauthorizedAccess:Lambda/TorRelay

Backdoor:Lambda/C&CActivity.B

Eine Lambda-Funktion fragt eine IP-Adresse ab, die einem bekannten Command-and-Control-Server zugeordnet wird.

Standard-Schweregrad: Hoch

- Feature: Lambda Network Activity Monitoring

Dieses Ergebnis informiert Sie darüber, dass eine aufgelistete Lambda-Funktion in Ihrer AWS Umgebung eine IP-Adresse abfragt, die einem bekannten Command-and-Control-Server (C&C) zugeordnet ist. Die mit der generierten Erkenntnis verknüpfte Lambda-Funktion ist möglicherweise kompromittiert. C&C-Server sind Computer, die Befehle an Mitglieder eines Botnets senden.

Ein Botnet ist eine Sammlung von mit dem Internet verbundenen Geräten, zu denen PCs, Server, mobile Geräte und Geräte des Internets der Dinge gehören können, die mit einem allgemeinen Typ von Malware infiziert sind und von dieser kontrolliert werden. Botnets dienen häufig zum Verteilen von Malware und zum Sammeln von sich widerrechtlich angeeigneten Informationen, wie z. B. Kreditkartennummern. Je nach Zweck und Struktur des Botnets kann der C&C-Server auch den Befehl erteilen, einen DDoS (Distributed Denial of Service)-Angriff zu starten.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, könnte Ihre Lambda-Funktion kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Lambda-Funktion.

CryptoCurrency:Lambda/BitcoinTool.B

Eine Lambda-Funktion fragt eine IP-Adresse ab, die mit einer Aktivität in Zusammenhang mit einer Kryptowährung in Verbindung steht.

Standard-Schweregrad: Hoch

- Feature: Lambda Network Activity Monitoring

Dieses Ergebnis informiert Sie darüber, dass die aufgelistete Lambda-Funktion in Ihrer AWS Umgebung eine IP-Adresse abfragt, die mit einer Bitcoin- oder anderen kryptowährungsbezogenen Aktivität verknüpft ist. Bedrohungsakteure versuchen möglicherweise, die Kontrolle über Lambda-Funktionen zu übernehmen, um sie böswillig für das unbefugte Mining von Kryptowährungen wiederzuverwenden.

Empfehlungen zur Abhilfe:

Wenn Sie diese Lambda-Funktion verwenden, um Kryptowährungen zu minen oder zu verwalten, oder wenn diese Funktion anderweitig an einer Blockchain-Aktivität beteiligt ist, handelt es sich möglicherweise um eine erwartete Aktivität für Ihre Umgebung. Wenn dies in Ihrer AWS Umgebung der Fall ist, empfehlen wir Ihnen, eine Unterdrückungsregel für dieses Ergebnis einzurichten.

Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Erkenntnistyp-Attribut mit dem Wert CryptoCurrency:Lambda/BitcoinTool.B verwenden. Das zweite Filterkriterium sollte der Lambda-Funktionsname des Features sein, die an der Blockchain-Aktivität beteiligt ist. Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln.

Wenn solche Aktivitäten unerwartet auftreten, könnte Ihre Lambda-Funktion kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Lambda-Funktion.

Trojan:Lambda/BlackholeTraffic

Die Lambda-Funktion versucht, mit einer IP-Adresse eines Remote-Hosts zu kommunizieren, der ein bekanntes schwarzes Loch ist.

Standard-Schweregrad: Mittel

- Feature: Lambda Network Activity Monitoring

Dieses Ergebnis informiert Sie darüber, dass eine aufgelistete Lambda-Funktion in Ihrer AWS Umgebung versucht, mit der IP-Adresse eines schwarzen Lochs (oder einer Senke) zu kommunizieren. Schwarze Löcher sind Stellen im Netzwerk, an denen eingehender oder ausgehender Datenverkehr stillschweigend verworfen wird, ohne die Quelle darüber zu informieren, dass die Daten den vorgesehenen Empfänger nicht erreicht haben. Die IP-Adresse eines schwarzen Lochs gibt einen Hostcomputer an, der nicht ausgeführt wird, oder eine Adresse, der kein Host zugewiesen wurde. Die aufgeführte Lambda-Funktion ist möglicherweise kompromittiert.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, könnte Ihre Lambda-Funktion kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Lambda-Funktion.

Trojan:Lambda/DropPoint

Eine Lambda-Funktion versucht, mit einer IP-Adresse eines Remote-Hosts zu kommunizieren, von dem bekannt ist, dass er Anmeldeinformationen und andere mithilfe von Malware gestohlene Daten enthält.

Standard-Schweregrad: Mittel

- Feature: Lambda Network Activity Monitoring

Dieses Ergebnis informiert Sie darüber, dass eine aufgelistete Lambda-Funktion in Ihrer AWS Umgebung versucht, mit der IP-Adresse eines Remote-Hosts zu kommunizieren, der bekanntermaßen Anmeldeinformationen und andere gestohlene Daten enthält, die von Malware erfasst wurden.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, könnte Ihre Lambda-Funktion kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Lambda-Funktion.

UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom

Eine Lambda-Funktion stellt Verbindungen zu einer IP-Adresse auf einer benutzerdefinierten Bedrohungsliste her.

Standard-Schweregrad: Mittel

- Feature: Lambda Network Activity Monitoring

Dieses Ergebnis informiert Sie darüber, dass eine Lambda-Funktion in Ihrer AWS Umgebung mit einer IP-Adresse kommuniziert, die in einer von Ihnen hochgeladenen Bedrohungsliste enthalten ist. In GuardDuty besteht eine Bedrohungsliste aus bekannten bösartigen IP-Adressen. GuardDuty generiert Ergebnisse auf der Grundlage der hochgeladenen Bedrohungslisten. Sie können die Details der Bedrohungsliste in den Funddetails auf der GuardDuty Konsole einsehen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, könnte Ihre Lambda-Funktion kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Lambda-Funktion.

UnauthorizedAccess:Lambda/TorClient

Eine Lambda-Funktion stellt Verbindungen zu einem Tor-Guard oder einem Authority-Knoten her.

Standard-Schweregrad: Hoch

- Feature: Lambda Network Activity Monitoring

Dieses Ergebnis informiert dich darüber, dass eine Lambda-Funktion in deiner AWS Umgebung Verbindungen zu einem Tor Guard- oder einem Authority-Knoten herstellt. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Tor-Guards und Authority-Knoten fungieren als erste Gateways in ein Tor-Netzwerk. Dieser Datenverkehr kann darauf hinweisen, dass diese Lambda-Funktion möglicherweise kompromittiert wurde. Sie fungiert jetzt als Client in einem Tor-Netzwerk.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, könnte Ihre Lambda-Funktion kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Lambda-Funktion.

UnauthorizedAccess:Lambda/TorRelay

Eine Lambda-Funktion stellt Verbindungen zu einem Tor-Netzwerk als Tor-Relay her.

Standard-Schweregrad: Hoch

- Feature: Lambda Network Activity Monitoring

Dieses Ergebnis informiert Sie darüber, dass eine Lambda-Funktion in Ihrer AWS Umgebung Verbindungen zu einem Tor-Netzwerk auf eine Weise herstellt, die darauf hindeutet, dass es als Tor-Relay fungiert. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Tor erhöht die Anonymität der Kommunikation, indem es den möglicherweise illegalen Datenverkehr des Kunden von einem Tor-Relay zu einem anderen weiterleitet.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, könnte Ihre Lambda-Funktion kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Lambda-Funktion.

GuardDuty Arten der Suche nach KI-Schutz

Wenn Sie AI Protection aktivieren, GuardDuty werden AWS CloudTrail Verwaltungsereignisse und Datenereignisse von Amazon Bedrock und Amazon SageMaker AI analysiert. GuardDuty verwendet diese Daten, um potenziell verdächtige Aktivitäten zu erkennen, die auf Ihre KI-Workloads abzielen. Wenn eine potenzielle Bedrohung GuardDuty erkannt wird, generiert es einen der folgenden

Erkennungstypen. Das `Resource type` für diese Ergebnisse ist`AccessKey`, und das Ergebnis identifiziert die IAM-Identität, die das Modell aufgerufen hat.

Jedes Ergebnis enthält auch Details zu den betroffenen KI-Ressourcen im `resource` Objekt des Ergebnisses. Zu den Impact:IAMUser/AnomalousModelInvocation Impact:IAMUser/CostHarvesting Ergebnissen gehört eine `resource.modelDetails` Liste, in der die aufgerufenen Amazon Bedrock- oder Amazon SageMaker AI-Modelle identifiziert werden. Der Impact:IAMUser/PromptInjection.Direct Fund beinhaltet ein `resource.bedrockGuardrailDetails` Objekt, das die Amazon Bedrock Guardrail beschreibt, die eingegriffen hat. Sie können diese Details in der GuardDuty Konsole oder im Finding-JSON einsehen.

Die Impact:IAMUser/AnomalousModelInvocation und Impact:IAMUser/CostHarvesting Findingtypen gelten sowohl für Amazon Bedrock- als auch für Amazon SageMaker AI-Modellaufrufe. Der Impact:IAMUser/PromptInjection.Direct Findetyp gilt für Amazon Bedrock-Workloads, die Amazon Bedrock Guardrails verwenden.

Themen

- Impact:IAMUser/AnomalousModelInvocation
- Impact:IAMUser/CostHarvesting
- Impact:IAMUser/PromptInjection.Direct

Impact:IAMUser/AnomalousModelInvocation

Eine IAM-Identität rief ein Amazon Bedrock- oder Amazon SageMaker AI-Modell auf eine Weise auf, die von der festgelegten Ausgangsbasis für die Identität oder das Konto abweicht.

Standard-Schweregrad: Niedrig

- Funktion: KI-Schutz

Dieses Ergebnis informiert Sie darüber, dass eine IAM-Identität ein Amazon Bedrock- oder Amazon SageMaker AI-Modell auf eine Weise aufgerufen hat, die von der historischen Aktivität der Identität oder des Kontos abweicht. Diese Aktivität könnte darauf hindeuten, dass ein Bedrohungsakteur kompromittierte Anmeldeinformationen verwendet, um auf Foundation-Modelle in Ihrem Konto zuzugreifen. Der Akteur könnte beispielsweise ein Modell untersuchen, gegnerische Eingaben vornehmen oder automatisierte Anfragen ausführen.

GuardDuty legt für jede IAM-Identität einen Basiswert für normale Modellaufrufaktivitäten AWS-Konto fest und ruft Amazon Bedrock oder Amazon AI auf. SageMaker GuardDuty erstellt Profile der Funktionen der Aufrufaktivität, einschließlich der folgenden:

- Die Modellaufruf-API, die die Identität aufgerufen hat
- Das Modell, das die Identität aufgerufen hat
- Die Quell-IP-Adresse und die zugehörige ASN-Organisation (Autonomous System Number)
- Der Benutzeragent, der die Abfrage gesendet hat

Wenn eine Aktivität GuardDuty beobachtet wird, die erheblich von diesem Ausgangswert abweicht, wird dieser Befund generiert. Beispiele hierfür sind Aufrufe von einer zuvor unbekannten IP-Adresse, einem zuvor unbekannten Benutzeragenten oder einem Modell, das die Identität nie aufgerufen hat. Das Ergebnis umfasst eine `resource.modelDetails` Liste, in der die Modelle identifiziert werden, die an der verdächtigen Aktivität beteiligt waren. Jeder Eintrag enthält einen ARN, der ein Amazon Bedrock Foundation-Modell, ein Inferenzprofil, ein bereitgestelltes, benutzerdefiniertes oder importiertes Modell, einen Amazon Bedrock Marketplace-Endpunkt, eine Prompt-Ressource oder einen Amazon SageMaker AI-Endpunktnamen `modelId` darstellt.

Dieses Ergebnis entspricht der MITRE ATLAS-Technik AML.T0040 — AI Model Inference API Access auf der MITRE ATLAS-Website.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

Um das Risiko unberechtigter Modellaufrufen zu verringern, sollten Sie einschränken, welche Identitäten Modelle aufrufen können. Beschränken Sie den Zugriff auf die folgenden Modellaufruf-APIs nur auf die Prinzipale und Modelle, für die sie erforderlich sind:

- `bedrock:InvokeModel`
- `bedrock:InvokeModelWithResponseStream`
- `bedrock:Converse`
- `bedrock:ConverseStream`
- `bedrock-mantle:CreateInference`

- `sagemaker:InvokeEndpoint`
- `sagemaker:InvokeEndpointAsync`
- `sagemaker:InvokeEndpointWithResponseStream`

Um Modellinferenzen in Ihrem Unternehmen zu verweigern, wo sie nicht benötigt werden, können Sie eine Service Control Policy (SCP) verwenden. Weitere Informationen finden Sie unter Identity-based Richtlinienbeispielen für Amazon Bedrock im Amazon Bedrock User Guide und Amazon SageMaker AI Identity-Based Policy Examples im Amazon SageMaker AI Developer Guide.

Impact:IAMUser/CostHarvesting

Eine IAM-Identität rief ein Amazon Bedrock- oder Amazon SageMaker AI-Modell mit anomalen Token-Volumen auf, was auf einen Cost-Harvesting-Angriff hindeuten könnte.

Standard-Schweregrad: Niedrig

- Funktion: KI-Schutz

Dieses Ergebnis informiert Sie darüber, dass eine IAM-Identität ein Amazon Bedrock- oder Amazon SageMaker AI-Modell mit Eingabe- oder Ausgabe-Token-Volumen aufgerufen hat, die erheblich vom Ausgangswert für die Identität oder das Konto abweichen. Bei einem Cost-Harvesting-Angriff sendet ein Bedrohungsakteur rechenintensive Eingaben an ein Modell, um die Betriebskosten des KI-Workloads in die Höhe zu treiben, ohne dabei unbedingt Daten zu exfiltrieren. Zu diesen Eingaben können übermäßig lange oder bewusst falsch formatierte Eingabeaufforderungen gehören.

GuardDuty legt für jede IAM-Identität und jedes Konto, das Amazon Bedrock- oder Amazon SageMaker AI-Modelle aufruft, eine Basislinie für das durchschnittliche Eingabe-Token-Volumen und das durchschnittliche Ausgabe-Token-Volumen fest. When GuardDuty beobachtet Aufrufe mit Token-Anzahlen, die diesen Basiswert überschreiten, und korreliert die Volumenanomalie mit anderen ungewöhnlichen Signalen, was zu diesem Ergebnis führt. GuardDuty Das Ergebnis berichtet über die anomale Aktivität im `service.detection` Objekt, einschließlich der beobachteten Aufrufe und Token-Volumina, die vom Ausgangswert abgewichen sind. Es enthält auch eine `resource.modelDetails` Liste, in der die Zielmodelle identifiziert werden. Jeder Eintrag enthält einen ARN, der ein Amazon Bedrock Foundation-Modell, ein Inferenzprofil, ein bereitgestelltes, benutzerdefiniertes oder importiertes Modell, einen Amazon Bedrock Marketplace-Endpunkt, eine Prompt-Ressource oder einen Amazon SageMaker AI-Endpunktnamen `modelId` darstellt.

Dieses Ergebnis entspricht der MITRE ATLAS-Technik AML.T0034 — Cost Harvesting auf der MITRE ATLAS-Website.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für die zugehörige Identität unerwartet ist, wurden die Anmeldeinformationen möglicherweise kompromittiert und verwendet, um die Kosten Ihrer KI-Workloads in die Höhe zu treiben. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten. Überprüfen Sie die mit der Identität verknüpften Modellaufrufe und beschränken Sie den Zugriff auf die betroffenen Modelle, indem Sie den Zugriff auf die folgenden Modellaufruf-APIs nur auf die Prinzipale beschränken, die sie benötigen:

- `bedrock:InvokeModel`
- `bedrock:InvokeModelWithResponseStream`
- `bedrock:Converse`
- `bedrock:ConverseStream`
- `bedrock-mantle:CreateInference`
- `sagemaker:InvokeEndpoint`
- `sagemaker:InvokeEndpointAsync`
- `sagemaker:InvokeEndpointWithResponseStream`

Um ungewöhnliche Ausgaben zu erkennen und einzudämmen, können Sie AWS Budgets verwenden, einschließlich Budgetaktionen, die bei Überschreitung eines Budgetschwellenwerts eine restriktive IAM-Richtlinie anwenden, und die Erkennung von Kostenanomalien.AWS Um Amazon Bedrock-Kosten bestimmten Workloads zuzuordnen, können Sie Kostenzuweisungs-Tags an ein Anwendungs-Inferenzprofil anhängen.

Impact:IAMUser/PromptInjection.Direct

Ein Amazon Bedrock Guardrail hat einen direkten Prompt-Injection-Versuch bei einem Aufruf durch eine IAM-Identität erkannt.

Standard-Schweregrad: Niedrig

- Funktion: KI-Schutz

Dieses Ergebnis informiert Sie darüber, dass ein Amazon Bedrock Guardrail, das für einen Amazon Bedrock-Workload in Ihrem Konto konfiguriert ist, einen direkten Prompt-Injection-Versuch erkannt hat. Bei einem Direct-Prompt-Injection-Angriff erstellt ein Bedrohungsakteur eine böswillige Aufforderung als Eingabe für ein Basismodell. Die Aufforderung veranlasst das Modell, seine ursprünglichen Anweisungen zu ignorieren und stattdessen den Anweisungen des Angreifers zu folgen. Eine Prompt Injection kann einem Angreifer ersten Zugriff gewähren, um zusätzliche Schritte gegen eine KI-Anwendung durchzuführen, wie etwa das Exfiltrieren von Daten, das Aufrufen nicht autorisierter Tools oder das Umgehen von Sicherheitskontrollen.

GuardDuty generiert dieses Ergebnis, wenn ein Amazon Bedrock Guardrail bei einem Aufruf eingreift, weil es einen sofortigen Angriff mit hoher Sicherheit erkannt hat. Um die Erkennung von Direct Prompt Injection GuardDuty zu aktivieren, konfigurieren Sie ein Amazon Bedrock Guardrail mit einem Inhaltsfilter für Prompt-Attacken. Um sicherzustellen, dass die Guardrail Aufrufe in Ihrer gesamten Umgebung auswertet, sollten Sie sie umfassend durchsetzen, anstatt sich darauf zu verlassen, dass einzelne Anwendungen sie an jede Anfrage anhängen. Sie können eine Guardrail für alle Aufrufe des Amazon Bedrock-Modells in einem Konto oder in Ihrer gesamten Organisation durchsetzen, indem Sie die Amazon Bedrock-Richtlinien unter verwenden. AWS OrganizationsWeitere Informationen finden Sie unter Anwenden kontenübergreifender Schutzmaßnahmen mit Amazon Bedrock Guardrails Enforcements im Amazon Bedrock-Benutzerhandbuch. Wenn eine Leitplanke einen Aufruf auswertet, zeichnet Amazon Bedrock die Auswertung in Form von AWS CloudTrail Datenereignissen auf, die dann GuardDuty analysiert werden, um dieses Ergebnis zu generieren.

Das Ergebnis beinhaltet ein `resource.bedrockGuardrailDetails` Objekt, das die Leitplanke beschreibt, die eingegriffen hat. In der folgenden Tabelle werden die Felder in diesem Objekt beschrieben.

Feld	Description
`guardrails`	Eine Liste der Leitplanken, die den Aufruf ausgewertet haben. Jeder Eintrag enthält den Amazon-Ressourcennamen (`arn`) und den Namen `version` der Leitplanke. Es können mehrere Guardrails auftreten, wenn ein und derselbe Aufruf sowohl durch ein Konto oder durch eine Organisation als auch durch eine Guardrail auf Anforderungsebene bewertet wird.
`guardrailAction`	Die Aktion, die die Leitplanke ergriffen hat. GuardDuty generiert diesen Befund, wenn der Wert `GUARDRAIL_INTERVENED`

Feld	Description
`guardrailSource`	Der Inhalt, den die Leitplanke ausgewertet hat. `INPUT`weist auf eine an das Modell gesendete Aufforderung und `OUTPUT` auf eine Antwort des Modells hin.
`contentPolicyFilters`	Eine Liste der Inhaltsrichtlinienfilter, die von der Leitplanke angewendet wurden. Für diesen Befundtyp hat ein Eintrag ein Von `type` `PROMPT_ATTACK` und ein `confidence` Von. `HIGH` Dies `action` ist der Fall, `BLOCKED` wenn die Guardrail den Inhalt blockiert hat oder `NONE` ob die Guardrail den Prompt-Angriff erkannt hat, aber nur so konfiguriert war, dass er gemeldet wird.

Dieser Befund entspricht der MITRE ATLAS-Technik AML.T0051 — LLM Prompt Injection auf der MITRE ATLAS-Website.

Empfehlungen zur Abhilfe:

Überprüfen Sie den Prompt, der die Guardrail-Intervention ausgelöst hat, und die IAM-Identität, die den Prompt gesendet hat. Wenn die Aktivität für die zugehörige Identität unerwartet ist, wurden die Anmeldeinformationen möglicherweise kompromittiert. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten. Wenn die Guardrail den Prompt-Angriff erkannt, aber nicht geblockt hat, sollten Sie in Erwägung ziehen, die Aktion des Inhaltsfilters „Prompt Attack“ auf Blockieren statt auf „Erkennen“ zu setzen, sodass die Guardrail den Inhalt blockiert. Weitere Informationen finden Sie unter Optionen für den Umgang mit schädlichen Inhalten, die von Amazon Bedrock Guardrails erkannt wurden, im Amazon Bedrock-Benutzerhandbuch. Sie können auch den Zugriff auf die Amazon Bedrock-Aufruf-APIs für die betroffene Identität einschränken.

Nicht mehr aktive Erkenntnistypen

Ein Ergebnis ist eine Benachrichtigung, die Details zu einem von GuardDuty festgestellten potenziellen Sicherheitsrisiko enthält. Informationen zu wichtigen Änderungen an den GuardDuty Befundtypen, einschließlich neu hinzugefügter oder veralteter Findtypen, finden Sie unterDokumentenverlauf für Amazon GuardDuty.

Die folgenden Befundtypen wurden eingestellt und nicht mehr von generiert GuardDuty.

> **Important**
>
> Sie können veraltete GuardDuty Findtypen nicht reaktivieren.

Themen

- PrivilegeEscalation:Kubernetes/PrivilegedContainer
- Persistence:Kubernetes/ContainerWithSensitiveMount
- Exfiltration:S3/ObjectRead.Unusual
- Impact:S3/PermissionsModification.Unusual
- Impact:S3/ObjectDelete.Unusual
- Discovery:S3/BucketEnumeration.Unusual
- Persistence:IAMUser/NetworkPermissions
- Persistence:IAMUser/ResourcePermissions
- Persistence:IAMUser/UserPermissions
- PrivilegeEscalation:IAMUser/AdministrativePermissions
- Recon:IAMUser/NetworkPermissions
- Recon:IAMUser/ResourcePermissions
- Recon:IAMUser/UserPermissions
- ResourceConsumption:IAMUser/ComputeResources
- Stealth:IAMUser/LoggingConfigurationModified
- UnauthorizedAccess:IAMUser/ConsoleLogin
- UnauthorizedAccess:EC2/TorIPCaller
- Backdoor:EC2/XORDDOS
- Behavior:IAMUser/InstanceLaunchUnusual
- CryptoCurrency:EC2/BitcoinTool.A
- UnauthorizedAccess:IAMUser/UnusualASNCaller

PrivilegeEscalation:Kubernetes/PrivilegedContainer

Ein privilegierter Container mit Zugriff auf Root-Ebene wurde auf Ihrem Kubernetes-Cluster gestartet.

Standard-Schweregrad: Mittel

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein privilegierter Container, der auf Ihrem Kubernetes-Cluster mithilfe eines Images gestartet wurde, das noch nie zuvor verwendet wurde, um privilegierte Container in Ihrem Cluster zu starten. Ein privilegierter Container hat Zugriff auf Root-Ebene auf den Host. Angreifer können als Taktik zur Erweiterung ihrer Rechte privilegierte Container starten, um sich Zugriff auf den Host zu verschaffen und ihn dann zu kompromittieren.

Empfehlungen zur Abhilfe:

Wenn dieser Container-Start unerwartet erfolgt, können die Anmeldeinformationen der Benutzeridentität, die zum Starten des Containers verwendet wurde, kompromittiert sein. Sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

Persistence:Kubernetes/ContainerWithSensitiveMount

Ein Container wurde gestartet, in dem ein sensibler externer Host-Pfad eingehängt war.

Standard-Schweregrad: Mittel

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein Container mit einer Konfiguration gestartet wurde, die im Abschnitt `volumeMounts` einen sensiblen Host-Pfad mit Schreibzugriff enthielt. Dadurch ist der sensible Host-Pfad vom Container aus zugänglich und beschreibbar. Diese Technik wird häufig von Gegnern verwendet, um Zugriff auf das Dateisystem des Hosts zu erhalten.

Empfehlungen zur Abhilfe:

Wenn dieser Container-Start unerwartet erfolgt, können die Anmeldeinformationen der Benutzeridentität, die zum Starten des Containers verwendet wurde, kompromittiert sein. Sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der EKS-Schutzfeststellungen.

Wenn dieser Container-Start erwartet wird, wird empfohlen, eine Unterdrückungsregel zu verwenden, die aus Filterkriterien besteht, die auf dem Feld `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix` basieren. In den Filterkriterien sollte das `imagePrefix`-Feld dem in der Erkenntnis angegebenen Feld `imagePrefix` entsprechen. Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln.

Exfiltration:S3/ObjectRead.Unusual

Eine IAM-Entität hat eine S3-API auf verdächtige Weise aufgerufen.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS Anmeldeinformationen aufgerufen wird, die auf einer Instance erstellt wurden, hat das Ergebnis den Schweregrad Hoch.

- Datenquelle: CloudTrail Datenereignisse für S3

Dieses Ergebnis informiert Sie darüber, dass eine IAM-Entität in Ihrer AWS Umgebung API-Aufrufe tätigt, die einen S3-Bucket betreffen und die sich von der festgelegten Baseline dieser Entität unterscheiden. Der in dieser Aktivität verwendete API-Aufruf steht im Zusammenhang mit der Exfiltrationsphase eines Angriffs, in der ein Angreifer versucht, Daten zu sammeln. Diese Aktivität ist verdächtig, da die Art und Weise, wie die IAM-Entität die API aufgerufen hat, ungewöhnlich war. Beispielsweise hatte diese IAM-Entität noch nie zuvor diese Art von API aufgerufen, oder die API wurde von einem ungewöhnlichen Ort aus aufgerufen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten S3-Buckets.

Impact:S3/PermissionsModification.Unusual

Eine IAM-Entität hat eine API aufgerufen, um die Berechtigungen für eine oder mehrere S3-Ressourcen zu ändern.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS Anmeldeinformationen aufgerufen wird, die auf einer Instance erstellt wurden, ist der Schweregrad des Ergebnisses hoch.

Diese Erkenntnis informiert Sie darüber, dass eine IAM-Entität API-Aufrufe durchführt, um die Berechtigungen für einen oder mehrere Buckets oder Objekte in Ihrer AWS -Umgebung zu ändern. Diese Aktion kann von einem Angreifer ausgeführt werden, um die Weitergabe von Informationen außerhalb des Kontos zu ermöglichen. Diese Aktivität ist verdächtig, da die Art und Weise, wie die IAM-Entität die API aufgerufen hat, ungewöhnlich war. Beispielsweise hatte diese IAM-Entität noch nie zuvor diese Art von API aufgerufen, oder die API wurde von einem ungewöhnlichen Ort aus aufgerufen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten S3-Buckets.

Impact:S3/ObjectDelete.Unusual

Eine IAM-Entität rief eine API zum Löschen von Daten in einem S3-Bucket auf.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS Anmeldeinformationen aufgerufen wird, die auf einer Instance erstellt wurden, hat das Ergebnis den Schweregrad Hoch.

Dieses Ergebnis informiert Sie darüber, dass eine bestimmte IAM-Entität in Ihrer AWS Umgebung API-Aufrufe durchführt, um Daten im aufgelisteten S3-Bucket zu löschen, indem der Bucket selbst gelöscht wird. Diese Aktivität ist verdächtig, da die Art und Weise, wie die IAM-Entität die API aufgerufen hat, ungewöhnlich war. Beispielsweise hatte diese IAM-Entität noch nie zuvor diese Art von API aufgerufen, oder die API wurde von einem ungewöhnlichen Ort aus aufgerufen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten S3-Buckets.

Discovery:S3/BucketEnumeration.Unusual

Eine IAM-Entität hat eine S3-API aufgerufen, um S3-Buckets in Ihrem Netzwerk zu erkennen.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS Anmeldeinformationen aufgerufen wird, die auf einer Instance erstellt wurden, ist der Schweregrad des Ergebnisses hoch.

Diese Erkenntnis informiert Sie darüber, dass eine IAM-Entität eine S3-API aufgerufen hat, um S3-Buckets in Ihrer Umgebung zu erkennen, z. B. `ListBuckets`. Diese Art von Aktivität steht im Zusammenhang mit der Erkennungsphase eines Angriffs, in der ein Angreifer Informationen sammelt, um festzustellen, ob Ihre AWS Umgebung für einen umfassenderen Angriff anfällig ist. Diese Aktivität

ist verdächtig, da die Art und Weise, wie die IAM-Entität die API aufgerufen hat, ungewöhnlich war. Beispielsweise hatte diese IAM-Entität noch nie zuvor diese Art von API aufgerufen, oder die API wurde von einem ungewöhnlichen Ort aus aufgerufen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell kompromittierten S3-Buckets.

Persistence:IAMUser/NetworkPermissions

Eine IAM-Entität hat eine API aufgerufen, die üblicherweise verwendet wird, um die Netzwerkzugriffsberechtigungen für Sicherheitsgruppen, Routen und ACLs in Ihrem AWS Konto.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS Anmeldeinformationen aufgerufen wird, die auf einer Instance erstellt wurden, hat das Ergebnis den Schweregrad Hoch.

Dieses Ergebnis deutet darauf hin, dass ein bestimmter Principal (Root-Benutzer des AWS-Kontos, eine IAM-Rolle oder ein bestimmter Benutzer) in Ihrer AWS Umgebung ein Verhalten zeigt, das sich von der festgelegten Ausgangslage unterscheidet. Dieser Prinzipal hat diese API bisher nicht aufgerufen.

Diese Erkenntnis wird ausgelöst, wenn Netzwerkkonfigurationseinstellungen unter verdächtigen Umständen geändert werden, z. B. wenn ein Prinzipal die `CreateSecurityGroup`-API aufruft, ohne dies jemals in der Vergangenheit getan zu haben. Angreifer versuchen häufig, Sicherheitsgruppen zu ändern, um bestimmten eingehenden Datenverkehr auf verschiedenen Ports zuzulassen und besser auf eine EC2-Instance zugreifen zu können.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

Persistence:IAMUser/ResourcePermissions

Ein Principal hat eine API aufgerufen, die üblicherweise verwendet wird, um die Sicherheitszugriffsrichtlinien verschiedener Ressourcen in Ihrem AWS-Konto.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die aufgerufene API jedoch temporäre AWS Anmeldeinformationen verwendet, die auf einer Instance erstellt wurden, hat das Ergebnis den Schweregrad Hoch.

Dieses Ergebnis deutet darauf hin, dass ein bestimmter Principal (Root-Benutzer des AWS-Kontos, eine IAM-Rolle oder ein bestimmter Benutzer) in Ihrer AWS Umgebung ein Verhalten zeigt, das sich von der festgelegten Baseline unterscheidet. Dieser Prinzipal hat diese API bisher nicht aufgerufen.

Dieses Ergebnis wird ausgelöst, wenn eine Änderung an Richtlinien oder Berechtigungen festgestellt wird, die mit AWS Ressourcen verknüpft sind, z. B. wenn ein Principal in Ihrer AWS Umgebung die `PutBucketPolicy` API aufruft, ohne dies in der Vergangenheit getan zu haben. Einige Services, z. B. Amazon S3, unterstützen ressourcengebundene Berechtigungen, die einem oder mehreren Prinzipalen Zugriff auf die Ressource gewähren. Mit gestohlenen Anmeldeinformationen können Angreifer die einer Ressource zugeordneten Richtlinien ändern, um sich künftig Zugriff auf diese Ressource zu verschaffen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

Persistence:IAMUser/UserPermissions

Ein Principal hat eine API aufgerufen, die üblicherweise zum Hinzufügen, Ändern oder Löschen von IAM-Benutzern, -Gruppen oder -Richtlinien in Ihrem AWS Konto.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS Anmeldeinformationen aufgerufen wird, die auf einer Instance erstellt wurden, hat das Ergebnis den Schweregrad Hoch.

Dieses Ergebnis deutet darauf hin, dass ein bestimmter Principal (Root-Benutzer des AWS-Kontos, eine IAM-Rolle oder ein bestimmter Benutzer) in Ihrer AWS Umgebung ein Verhalten zeigt, das sich von der festgelegten Ausgangslage unterscheidet. Dieser Prinzipal hat diese API bisher nicht aufgerufen.

Dieses Ergebnis wird durch verdächtige Änderungen an den benutzerbezogenen Berechtigungen in Ihrer AWS Umgebung ausgelöst, z. B. wenn ein Principal in Ihrer AWS Umgebung die `AttachUserPolicy` API aufruft, ohne dies in der Vergangenheit getan zu haben. Angreifer können gestohlene Anmeldeinformationen verwenden, um neue Benutzer zu erstellen, Zugriffsrichtlinien für bestehende Benutzer hinzuzufügen oder Zugriffsschlüssel zu erstellen, um ihren Zugriff auf ein Konto zu maximieren, selbst wenn ihr ursprünglicher Zugangspunkt geschlossen ist. Beispielsweise könnte der Besitzer des Kontos feststellen, dass ein bestimmter IAM-Benutzer oder ein bestimmtes IAM-Passwort gestohlen wurde, und es aus dem Konto löschen. Andere Benutzer, die von einem betrügerisch erstellten Administratorprinzipal erstellt wurden, werden jedoch möglicherweise nicht gelöscht, sodass der Angreifer auf ihr AWS Konto zugreifen kann.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

PrivilegeEscalation:IAMUser/AdministrativePermissions

Ein Prinzipal hat versucht, sich selbst eine hochgradig weitreichende Richtlinie zuzuweisen.

Standard-Schweregrad: Niedrig*

> **Note**
>
> Wenn der Angriff auf die Berechtigungseskalation nicht erfolgreich war, ist der Schweregrad des Ergebnisses „Niedrig“, wenn der Angriff erfolgreich war, ist der Schweregrad „Mittel“.

Dieses Ergebnis deutet darauf hin, dass eine bestimmte IAM-Entität in Ihrer AWS Umgebung ein Verhalten zeigt, das auf einen Angriff zur Eskalation von Rechten hinweisen kann. Diese Erkenntnis wird ausgelöst, wenn ein IAM-Benutzer oder eine Rolle versucht, sich selbst eine hochgradig weitreichende Richtlinie zuzuweisen. Wenn der betreffende Benutzer oder die betreffende Rolle nicht über Administratorrechte verfügen soll, sind entweder die Anmeldeinformationen des Benutzers gefährdet oder die Berechtigungen der Rolle sind möglicherweise nicht richtig konfiguriert.

Angreifer können gestohlene Anmeldeinformationen verwenden, um neue Benutzer zu erstellen, Zugriffsrichtlinien für bestehende Benutzer hinzuzufügen oder Zugriffsschlüssel zu erstellen, um ihren Zugriff auf ein Konto zu maximieren, selbst wenn ihr ursprünglicher Zugangspunkt geschlossen ist. Der Eigentümer des Kontos stellt möglicherweise fest, dass ein bestimmter IAM-Benutzer oder ein Passwort gestohlen wurden, und löscht diese aus dem Konto. Hierbei entfernt er aber möglicherweise andere Benutzer nicht, die vom betrügerisch angelegten Admin-Prinzipal angelegt wurden, sodass ihr AWS -Konto dem Angreifer weiterhin zur Verfügung steht.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

Recon:IAMUser/NetworkPermissions

Ein Principal hat eine API aufgerufen, die üblicherweise verwendet wird, um die Netzwerkzugriffsberechtigungen für Sicherheitsgruppen, Routen und ACLs in Ihrem AWS Konto.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS Anmeldeinformationen aufgerufen wird, die auf einer Instance erstellt wurden, hat das Ergebnis den Schweregrad Hoch.

Dieses Ergebnis deutet darauf hin, dass ein bestimmter Principal (Root-Benutzer des AWS-Kontos, eine IAM-Rolle oder ein bestimmter Benutzer) in Ihrer AWS Umgebung ein Verhalten zeigt, das sich von der festgelegten Ausgangslage unterscheidet. Dieser Prinzipal hat diese API bisher nicht aufgerufen.

Diese Erkenntnis wird ausgelöst, wenn Ressourcen-Zugriffsberechtigungen in Ihrem AWS -Konto unter fragwürdigen Umständen untersucht werden. Dies trifft beispielsweise dann zu, wenn ein Prinzipal zum ersten Mal die `DescribeInstances`-API aufgerufen hat. Ein Angreifer könnte gestohlene Anmeldeinformationen verwenden, um diese Art der Erkennung Ihrer AWS Ressourcen durchzuführen, um wertvollere Anmeldeinformationen zu finden oder die Fähigkeiten der Anmeldeinformationen zu ermitteln, über die er bereits verfügt.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

Recon:IAMUser/ResourcePermissions

Ein Principal hat eine API aufgerufen, die üblicherweise verwendet wird, um die Sicherheitszugriffsrichtlinien verschiedener Ressourcen in Ihrem AWS Konto.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS Anmeldeinformationen aufgerufen wird, die auf einer Instance erstellt wurden, hat das Ergebnis den Schweregrad Hoch.

Dieses Ergebnis deutet darauf hin, dass ein bestimmter Principal (Root-Benutzer des AWS-Kontos, eine IAM-Rolle oder ein bestimmter Benutzer) in Ihrer AWS Umgebung ein Verhalten zeigt, das sich von der festgelegten Ausgangslage unterscheidet. Dieser Prinzipal hat diese API bisher nicht aufgerufen.

Diese Erkenntnis wird ausgelöst, wenn Ressourcen-Zugriffsberechtigungen in Ihrem AWS -Konto unter fragwürdigen Umständen untersucht werden. Dies trifft beispielsweise dann zu, wenn ein Prinzipal zum ersten Mal die `DescribeInstances`-API aufgerufen hat. Ein Angreifer könnte gestohlene Anmeldeinformationen verwenden, um diese Art der Erkennung Ihrer AWS Ressourcen durchzuführen, um wertvollere Anmeldeinformationen zu finden oder die Fähigkeiten der Anmeldeinformationen zu ermitteln, über die er bereits verfügt.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

Recon:IAMUser/UserPermissions

Ein Principal hat eine API aufgerufen, die üblicherweise zum Hinzufügen, Ändern oder Löschen von IAM-Benutzern, -Gruppen oder -Richtlinien in Ihrem AWS Konto.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS Anmeldeinformationen aufgerufen wird, die auf einer Instance erstellt wurden, hat das Ergebnis den Schweregrad Hoch.

Dieses Ergebnis wird ausgelöst, wenn Benutzerberechtigungen in Ihrer AWS Umgebung unter verdächtigen Umständen geprüft werden. Dies trifft beispielsweise dann zu, wenn ein Prinzipal (Root-Benutzer des AWS-Kontos, IAM-Rolle, oder Benutzer) zum ersten Mal die `ListInstanceProfilesForRole`-API aufgerufen hat. Ein Angreifer könnte gestohlene Anmeldeinformationen verwenden, um diese Art der Erkennung Ihrer AWS Ressourcen durchzuführen, um wertvollere Anmeldeinformationen zu finden oder die Fähigkeiten der Anmeldeinformationen zu ermitteln, über die er bereits verfügt.

Dieses Ergebnis deutet darauf hin, dass ein bestimmter Principal in Ihrer AWS Umgebung ein Verhalten zeigt, das sich von der festgelegten Ausgangslage unterscheidet. Dieser Prinzipal hat diese API bisher nicht aufgerufen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

ResourceConsumption:IAMUser/ComputeResources

Ein Prinzipal hat eine API aufgerufen, die häufig zum Starten von Datenverarbeitungsressourcen verwendet wird, wie beispielsweise EC2-Instances.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS Anmeldeinformationen aufgerufen wird, die auf einer Instance erstellt wurden, hat das Ergebnis den Schweregrad Hoch.

Diese Erkenntnis wird ausgelöst, wenn EC2-Instances im aufgeführten Konto in Ihrer AWS -Umgebung unter fragwürdigen Umständen gestartet werden. Dieses Ergebnis deutet darauf hin, dass ein bestimmter Principal in Ihrer AWS Umgebung ein Verhalten zeigt, das sich von der festgelegten Baseline unterscheidet, z. B. wenn ein Principal (Root-Benutzer des AWS-Kontos, eine IAM-Rolle oder ein IAM-Benutzer) die `RunInstances` API aufgerufen hat, ohne dies in der Vergangenheit getan zu haben. Dies kann ein Anzeichen für einen Angreifer sein, der gestohlene Anmeldeinformationen nutzt, um Rechenzeit zu stehlen (beispielsweise für das Mining von

Kryptowährung oder zum Entschlüsseln von Passwörtern). Es kann auch ein Hinweis darauf sein, dass ein Angreifer eine EC2-Instance in Ihrer AWS Umgebung und deren Anmeldeinformationen verwendet, um den Zugriff auf Ihr Konto aufrechtzuerhalten.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

Stealth:IAMUser/LoggingConfigurationModified

Ein Principal hat eine API aufgerufen, die üblicherweise verwendet wird, um die CloudTrail Protokollierung zu beenden, bestehende Protokolle zu löschen und auf andere Weise Spuren von Aktivitäten in Ihrem AWS Konto.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS Anmeldeinformationen aufgerufen wird, die auf einer Instance erstellt wurden, hat das Ergebnis den Schweregrad Hoch.

Diese Erkenntnis wird ausgelöst, wenn die Protokollierungskonfiguration in dem aufgeführten AWS -Konto in Ihrer Umgebung unter fragwürdigen Umständen geändert wird. Dieses Ergebnis informiert Sie darüber, dass ein bestimmter Principal in Ihrer AWS Umgebung ein Verhalten zeigt, das sich von der festgelegten Baseline unterscheidet, z. B. wenn ein Principal (Root-Benutzer des AWS-Kontos, eine IAM-Rolle oder ein IAM-Benutzer) die `StopLogging` API aufgerufen hat, ohne dies in der Vergangenheit getan zu haben. Dies kann darauf hinweisen, dass ein Angreifer versucht, seine Spuren zu verwischen, indem er alle Anzeichen von Aktivität entfernt.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

UnauthorizedAccess:IAMUser/ConsoleLogin

Eine ungewöhnliche Konsolenanmeldung durch einen Principal in Ihrem AWS Konto wurde beobachtet.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS Anmeldeinformationen aufgerufen wird, die auf einer Instance erstellt wurden, hat das Ergebnis den Schweregrad Hoch.

Diese Erkenntnis wird ausgelöst, wenn eine Konsolenanmeldung unter fragwürdigen Umständen erkannt wird. Dies ist beispielsweise der Fall, wenn ein Principal, der dies in der Vergangenheit noch nicht getan hat, die ConsoleLogin API von einem Client aus aufgerufen hat, der noch nie zuvor verwendet wurde, oder von einem ungewöhnlichen Standort aus. Dies könnte ein Hinweis darauf sein, dass gestohlene Anmeldeinformationen verwendet wurden, um auf Ihr AWS Konto zuzugreifen, oder dass ein gültiger Benutzer auf ungültige oder weniger sichere Weise auf das Konto zugreift (z. B. nicht über ein zugelassenes VPN).

Dieses Ergebnis informiert Sie darüber, dass ein bestimmter Principal in Ihrer AWS Umgebung ein Verhalten zeigt, das sich von der festgelegten Ausgangslage unterscheidet. Für diesen Prinzipal gibt es keinen vorherigen Verlauf von Anmeldeaktivitäten mit dieser Client-Anwendung von diesem bestimmten Standort aus.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

UnauthorizedAccess:EC2/TorIPCaller

Ihre EC2-Instance erhält eingehende Verbindungen von einem Tor-Exit-Knoten.

Standard-Schweregrad: Mittel

Dieses Ergebnis informiert Sie darüber, dass eine EC2-Instance in Ihrer AWS Umgebung eingehende Verbindungen von einem Tor-Ausgangsknoten empfängt. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese nach dem Zufallsprinzip durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Dieses Ergebnis kann auf einen unbefugten Zugriff auf Ihre AWS Ressourcen hinweisen, mit der Absicht, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Backdoor:EC2/XORDDOS

Eine EC2-Instance versucht, mit einer IP-Adresse zu kommunizieren, die mit XOR-DDoS-Malware in Verbindung steht.

Standard-Schweregrad: Hoch

Dieses Ergebnis informiert Sie darüber, dass eine EC2-Instance in Ihrer AWS Umgebung versucht, mit einer IP-Adresse zu kommunizieren, die mit XOR-DDoS-Malware in Verbindung steht. Diese EC2-Instance wurde möglicherweise kompromittiert. XOR DDoS ist eine Trojaner-Malware, die Linux-Systeme kapert. Sie versucht Zugriff auf das System zu erhalten, indem sie einen Brute-Force-Angriff startet, um das Passwort für Secure Shell (SSH)-Services unter Linux zu ermitteln. Nachdem die SSH-Anmeldeinformationen erlangt wurden und die Anmeldung erfolgreich war, wird ein Skript mit Root-Berechtigungen ausgeführt, um XOR DDoS herunterzuladen und zu installieren. Diese Malware wird dann als Teil eines Botnets verwendet, um verteilte Distributed Denial of Service (DDoS)-Angriffe auf andere Ziele durchzuführen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

Behavior:IAMUser/InstanceLaunchUnusual

Ein Benutzer hat eine EC2-Instance eines ungewöhnlichen Typs gestartet.

Standard-Schweregrad: Hoch

Dieses Ergebnis informiert Sie darüber, dass ein bestimmter Benutzer in Ihrer AWS Umgebung ein Verhalten zeigt, das sich von der festgelegten Ausgangslage unterscheidet. Dieser Benutzer hat noch nie zuvor eine EC2-Instance dieses Typs gestartet. Ihre Anmeldeinformationen wurden möglicherweise kompromittiert.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

CryptoCurrency:EC2/BitcoinTool.A

Eine EC2-Instance kommuniziert mit Bitcoin-Mining-Pools.

Standard-Schweregrad: Hoch

Dieses Ergebnis informiert Sie darüber, dass eine EC2-Instance in Ihrer AWS Umgebung mit Bitcoin-Mining-Pools kommuniziert. Beim Mining von Kryptowährungen werden Ressourcen in einem Pool kombiniert, damit die Verarbeitungsleistung über ein Netzwerk gemeinsam genutzt werden kann. Der Gewinn wird dann nach Maßgabe der zur Lösung des Blocks beigetragenen Arbeit aufgeteilt. Wenn Sie diese EC2-Instance nicht für Bitcoin-Mining verwenden, könnte Ihre EC2-Instance kompromittiert worden sein.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

UnauthorizedAccess:IAMUser/UnusualASNCaller

Eine API wurde von einer IP-Adresse eines unüblichen Netzwerks aufgerufen.

Standard-Schweregrad: Hoch

Dieses Ergebnis informiert Sie darüber, dass eine bestimmte Aktivität von einer IP-Adresse eines ungewöhnlichen Netzwerks aus aufgerufen wurde. Dieses Netzwerk wurde im gesamten AWS -Nutzungsverlauf des beschriebenen Benutzers noch nie beobachtet. Diese Aktivität kann eine Konsolen-Anmeldung, einen Versuch, eine EC2-Instance zu starten, einen neuen IAM-Benutzer anzulegen, Ihre AWS -Privilegien zu ändern usw. beinhalten. Dies kann auf einen unbefugten Zugriff auf Ihre AWS Ressourcen hinweisen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.

GuardDuty Suchen nach Typen anhand potenziell betroffener Ressourcen

Die folgenden Seiten sind nach dem Typ der potenziell betroffenen Ressource, die mit einem GuardDuty Ergebnis verknüpft ist, kategorisiert:

- EC2-Erkenntnistypen
- IAM-Erkenntnistypen
- Arten der Suche nach Angriffssequenzen
- S3-Schutztypen finden
- Arten der Suche nach EKS-Schutz
- Bei der Laufzeitüberwachung werden Typen gefunden
- Malware-Schutz für EC2-Suchtypen
- Suchtyp „Malware-Schutz für S3“
- Malware-Schutz für Backup-Suchtypen
- Erkenntnistypen für RDS Protection
- Lambda-Protection-Erkenntnistypen
- Arten der Suche nach KI-Schutz

GuardDuty Typen von aktiven Ergebnissen

Die folgende Tabelle zeigt alle aktiven Findetypen, gruppiert nach ihrer Quelle: zuerst die Findetypen aus der grundlegenden Bedrohungserkennung (sortiert nach Datenquelle), dann die Erkennungstypen der Erweiterte Bedrohungserkennung Angriffssequenz und dann die Erkennungstypen aus den einzelnen Schutzplänen (in alphabetischer Reihenfolge nach Plan). In der folgenden Tabelle sind die Werte in der Spalte „Schweregrad“ einiger Ergebnisse mit einem Sternchen (*) oder einem Pluszeichen (+) gekennzeichnet:

* Diese Ergebnisarten haben einen unterschiedlichen Schweregrad. Ein Befund eines bestimmten Typs kann je nach dem für das Ergebnis spezifischen Kontext einen unterschiedlichen Schweregrad haben. Weitere Informationen zu einem Befundtyp finden Sie in der ausführlichen Beschreibung.

+ EC2-Ergebnisse, die VPC-Flow-Logs als Datenquelle verwenden, unterstützen keinen IPv6-Verkehr.

Ergebnistyp	Ressourcentyp	Grundlegende Daten source/Feature	Der Schweregrad einer Erkenntnis
CredentialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail Management-Ereignisse	Mittel
DefenseEvasion:IAMUser/AnomalousBehavior	IAM	CloudTrail Management-Ereignisse	Mittel
DefenseEvasion:IAMUser/BedrockLoggingDisabled	IAM	CloudTrail Management-Ereignisse	Mittel
Discovery:IAMUser/AnomalousBehavior	IAM	CloudTrail Management-Ereignisse	Niedrig
Exfiltration:IAMUser/AnomalousBehavior	IAM	CloudTrail Management-Ereignisse	Hoch
Impact:IAMUser/AnomalousBehavior	IAM	CloudTrail Management-Ereignisse	Hoch
InitialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail Management-Ereignisse	Mittel

Ergebnistyp	Ressourcentyp	Grundlegende Daten source/Feature	Der Schweregrad einer Erkenntnis
PenTest:IAMUser/KaliLinux	IAM	CloudTrail Management-Ereignisse	Mittel
PenTest:IAMUser/ParrotLinux	IAM	CloudTrail Management-Ereignisse	Mittel
PenTest:IAMUser/PentooLinux	IAM	CloudTrail Management-Ereignisse	Mittel
Persistence:IAMUser/AnomalousBehavior	IAM	CloudTrail Management-Ereignisse	Mittel
Stealth:IAMUser/PasswordPolicyChange	IAM	CloudTrail Management-Ereignisse	Niedrig *
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	IAM	CloudTrail Management-Ereignisse	Hoch *
Policy:S3/AccountBlockPublicAccessDisabled	Amazon S3	CloudTrail Management-Ereignisse	Niedrig
Policy:S3/BucketAnonymousAccessGranted	Amazon S3	CloudTrail Management-Ereignisse	Hoch
Policy:S3/BucketBlockPublicAccessDisabled	Amazon S3	CloudTrail Management-Ereignisse	Niedrig

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Policy:S3/BucketPublicAccessGranted	Amazon S3	CloudTrail Management-Ereignisse	Hoch
PrivilegeEscalation:IAMUser/AnomalousBehavior	IAM	CloudTrail Management-Ereignisse	Mittel
Recon:IAMUser/MaliciousIPCaller	IAM	CloudTrail Management-Ereignisse	Mittel
Recon:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail Management-Ereignisse	Mittel
Recon:IAMUser/TorIPCaller	IAM	CloudTrail Management-Ereignisse	Mittel
Stealth:IAMUser/CloudTrailLoggingDisabled	IAM	CloudTrail Management-Ereignisse	Niedrig
Stealth:S3/ServerAccessLoggingDisabled	Amazon S3	CloudTrail Management-Ereignisse	Niedrig
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	IAM	CloudTrail Management-Ereignisse	Mittel
UnauthorizedAccess:IAMUser/MaliciousIPCaller	IAM	CloudTrail Management-Ereignisse	Mittel

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail Management-Ereignisse	Mittel
UnauthorizedAccess:IAMUser/TorIPCaller	IAM	CloudTrail Management-Ereignisse	Mittel
CredentialAccess:IAMUser/CompromisedCredentials	IAM	CloudTrail Verwaltungsereignisse oder CloudTrail Datenereignisse für S3	Hoch
Policy:IAMUser/RootCredentialUsage	IAM	CloudTrail Verwaltungsereignisse oder CloudTrail Datenereignisse für S3	Niedrig
Policy:IAMUser/ShortTermRootCredentialUsage	IAM	CloudTrail Verwaltungsereignisse oder CloudTrail Datenereignisse für S3	Niedrig
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	IAM	CloudTrail Verwaltungsereignisse oder CloudTrail Datenereignisse für S3	Hoch
UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS	IAM	CloudTrail Verwaltungsereignisse	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS	IAM	CloudTrail Verwaltungsereignisse oder CloudTrail Datenereignisse für S3	Hoch
Impact:EC2/MaliciousDomainRequest.Custom	Amazon EC2	DNS-Protokolle	Mittel
Backdoor:EC2/C&CActivity.B!DNS	Amazon EC2	DNS-Protokolle	Hoch
CryptoCurrency:EC2/BitcoinTool.B!DNS	Amazon EC2	DNS-Protokolle	Hoch
Impact:EC2/AbusedDomainRequest.Reputation	Amazon EC2	DNS-Protokolle	Mittel
Impact:EC2/BitcoinDomainRequest.Reputation	Amazon EC2	DNS-Protokolle	Hoch
Impact:EC2/MaliciousDomainRequest.Reputation	Amazon EC2	DNS-Protokolle	Hoch
Impact:EC2/SuspiciousDomainRequest.Reputation	Amazon EC2	DNS-Protokolle	Niedrig
Trojan:EC2/BlackholeTraffic!DNS	Amazon EC2	DNS-Protokolle	Mittel

Ergebnistyp	Ressourcentyp	Grundlegende Daten source/Feature	Der Schweregrad einer Erkenntnis
Trojan:EC2/DGADomainRequest.B	Amazon EC2	DNS-Protokolle	Hoch
Trojan:EC2/DGADomainRequest.C!DNS	Amazon EC2	DNS-Protokolle	Hoch
Trojan:EC2/DNSDataExfiltration	Amazon EC2	DNS-Protokolle	Hoch
Trojan:EC2/DriveBySourceTraffic!DNS	Amazon EC2	DNS-Protokolle	Hoch
Trojan:EC2/DropPoint!DNS	Amazon EC2	DNS-Protokolle	Mittel
Trojan:EC2/PhishingDomainRequest!DNS	Amazon EC2	DNS-Protokolle	Hoch
UnauthorizedAccess:EC2/MetadataDNSRebind	Amazon EC2	DNS-Protokolle	Hoch
Backdoor:EC2/C&CActivity.B	Amazon EC2	VPC-Flussprotokolle ±	Hoch
Backdoor:EC2/DenialOfService.Dns	Amazon EC2	VPC-Flussprotokolle ±	Hoch
Backdoor:EC2/DenialOfService.Tcp	Amazon EC2	VPC-Flussprotokolle ±	Hoch
Backdoor:EC2/DenialOfService.Udp	Amazon EC2	VPC-Flussprotokolle ±	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Daten source/Feature	Der Schweregrad einer Erkenntnis
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	Amazon EC2	VPC-Flussprotokolle [+]	Hoch
Backdoor:EC2/DenialOfService.UnusualProtocol	Amazon EC2	VPC-Flussprotokolle [+]	Hoch
Backdoor:EC2/Spambot	Amazon EC2	VPC-Flussprotokolle [+]	Mittel
Behavior:EC2/NetworkPortUnusual	Amazon EC2	VPC-Flussprotokolle [+]	Mittel
Behavior:EC2/TrafficVolumeUnusual	Amazon EC2	VPC-Flussprotokolle [+]	Mittel
CryptoCurrency:EC2/BitcoinTool.B	Amazon EC2	VPC-Flussprotokolle [+]	Hoch
DefenseEvasion:EC2/UnusualDNSResolver	Amazon EC2	VPC-Flussprotokolle [+]	Mittel
DefenseEvasion:EC2/UnusualDoHActivity	Amazon EC2	VPC-Flussprotokolle [+]	Mittel
DefenseEvasion:EC2/UnusualDoTActivity	Amazon EC2	VPC-Flussprotokolle [+]	Mittel
Impact:EC2/PortSweep	Amazon EC2	VPC-Flussprotokolle [+]	Hoch
Impact:EC2/WinRMBruteForce	Amazon EC2	VPC-Flussprotokolle [+]	Niedrig [*]

Ergebnistyp	Ressourcentyp	Grundlegende Daten source/Feature	Der Schweregrad einer Erkenntnis
Recon:EC2/PortProbeEMRUnprotectedPort	Amazon EC2	VPC-Flussprotokolle +	Hoch
Recon:EC2/PortProbeUnprotectedPort	Amazon EC2	VPC-Flussprotokolle +	Niedrig *
Recon:EC2/Portscan	Amazon EC2	VPC-Flussprotokolle +	Mittel
Trojan:EC2/BlackholeTraffic	Amazon EC2	VPC-Flussprotokolle +	Mittel
Trojan:EC2/DropPoint	Amazon EC2	VPC-Flussprotokolle +	Mittel
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	Amazon EC2	VPC-Flussprotokolle +	Mittel
UnauthorizedAccess:EC2/RDPBruteForce	Amazon EC2	VPC-Flussprotokolle +	Niedrig *
UnauthorizedAccess:EC2/SSHBruteForce	Amazon EC2	VPC-Flussprotokolle +	Niedrig *
UnauthorizedAccess:EC2/TorClient	Amazon EC2	VPC-Flussprotokolle +	Hoch
UnauthorizedAccess:EC2/TorRelay	Amazon EC2	VPC-Flussprotokolle +	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Daten source/Feature	Der Schweregrad einer Erkenntnis
AttackSequence:EKS/CompromisedCluster	An der Angriffss equenz beteiligte Ressourcen	• EKS-Auditprotokoll ereignisse • Laufzeitüberwachun g für Amazon EKS • Amazon EKS-Malware-Erkennung für Amazon EC2 • AWS CloudTrail Datenereignisse für S3 • AWS CloudTrail Verwaltungsereigni sse • VPC Flow Logs • Route53 Resolver DNS-Abfra geprotokolle	Kritisch
AttackSequence:IAM/CompromisedCreden tials	An der Angriffss equenz beteiligte Ressourcen	CloudTrail Verwaltun gsereignisse	Kritisch
AttackSequence:S3/CompromisedData	An der Angriffss equenz beteiligte Ressourcen	CloudTrail Verwaltun gsereignisse und CloudTrail Datenerei gnisse für S3	Kritisch

Ergebnistyp	Ressourcentyp	Grundlegende Daten source/Feature	Der Schweregrad einer Erkenntnis
AttackSequence:ECS/CompromisedCluster	An der Angriffss equenz beteiligte Ressourcen	• AWS Amazon ECS Runtime-Erkennungen (Fargate) • AWS Amazon ECS-Runtime-Erkennungen (Amazon EC2 EC2-Instances) • AWS Malware-Erkennungen	Kritisch
AttackSequence:EC2/CompromisedInstanceGroup	An der Angriffss equenz beteiligte Ressourcen	• AWS Amazon EC2 Runtime-Erkennungen • AWS Malware-Erkennungen • VPC Flow Logs • Route53 Resolver DNS-Abfrageprotokolle	Kritisch
Impact:IAMUser/AnomalousModelInvocation	IAM	KI-Schutz	Niedrig
Impact:IAMUser/CostHarvesting	IAM	KI-Schutz	Niedrig
Impact:IAMUser/PromptInjection.Direct	IAM	KI-Schutz	Niedrig

Ergebnistyp	Ressourcentyp	Grundlegende Daten source/Feature	Der Schweregrad einer Erkenntnis
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	Kubernetes	EKS-Auditprotokolle	Mittel
CredentialAccess:Kubernetes/MaliciousIPCaller	Kubernetes	EKS-Auditprotokolle	Hoch
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKS-Auditprotokolle	Hoch
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKS-Auditprotokolle	Hoch
CredentialAccess:Kubernetes/TorIPCaller	Kubernetes	EKS-Auditprotokolle	Hoch
DefenseEvasion:Kubernetes/MaliciousIPCaller	Kubernetes	EKS-Auditprotokolle	Hoch
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKS-Auditprotokolle	Hoch
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKS-Auditprotokolle	Hoch
DefenseEvasion:Kubernetes/TorIPCaller	Kubernetes	EKS-Auditprotokolle	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Daten source/Feature	Der Schweregrad einer Erkenntnis
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	Kubernetes	EKS-Auditprotokolle	Niedrig
Discovery:Kubernetes/MaliciousIPCaller	Kubernetes	EKS-Auditprotokolle	Mittel
Discovery:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKS-Auditprotokolle	Mittel
Discovery:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKS-Auditprotokolle	Mittel
Discovery:Kubernetes/TorIPCaller	Kubernetes	EKS-Auditprotokolle	Mittel
Execution:Kubernetes/ExecInKubeSystemPod	Kubernetes	EKS-Auditprotokolle	Mittel
Execution:Kubernetes/AnomalousBehavior.ExecInPod	Kubernetes	EKS-Auditprotokolle	Mittel
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	Kubernetes	EKS-Auditprotokolle	Niedrig
Impact:Kubernetes/MaliciousIPCaller	Kubernetes	EKS-Auditprotokolle	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Daten source/Feature	Der Schweregrad einer Erkenntnis
Impact:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKS-Auditprotokolle	Hoch
Impact:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKS-Auditprotokolle	Hoch
Impact:Kubernetes/TorIPCaller	Kubernetes	EKS-Auditprotokolle	Hoch
Persistence:Kubernetes/MaliciousIPCaller	Kubernetes	EKS-Auditprotokolle	Mittel
Persistence:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKS-Auditprotokolle	Mittel
Persistence:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKS-Auditprotokolle	Hoch
Persistence:Kubernetes/TorIPCaller	Kubernetes	EKS-Auditprotokolle	Mittel
Policy:Kubernetes/AdminAccessToDefaultServiceAccount	Kubernetes	EKS-Auditprotokolle	Hoch
Policy:Kubernetes/AnonymousAccessGranted	Kubernetes	EKS-Auditprotokolle	Hoch
Policy:Kubernetes/KubeflowDashboardExposed	Kubernetes	EKS-Auditprotokolle	Mittel

Ergebnistyp	Ressourcentyp	Grundlegende Daten source/Feature	Der Schweregrad einer Erkenntnis
Policy:Kubernetes/ExposedDashboard	Kubernetes	EKS-Auditprotokolle	Mittel
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	Kubernetes	EKS-Auditprotokolle	Mittel *
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	Kubernetes	EKS-Auditprotokolle	Niedrig
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	Kubernetes	EKS-Auditprotokolle	Hoch
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	Kubernetes	EKS-Auditprotokolle	Hoch
Backdoor:Lambda/C&CActivity.B	Lambda	Lambda Network Activity Monitoring	Hoch
CryptoCurrency:Lambda/BitcoinTool.B	Lambda	Lambda Network Activity Monitoring	Hoch
Trojan:Lambda/BlackholeTraffic	Lambda	Lambda Network Activity Monitoring	Mittel
Trojan:Lambda/DropPoint	Lambda	Lambda Network Activity Monitoring	Mittel

Ergebnistyp	Ressourcentyp	Grundlegende Daten source/Feature	Der Schweregrad einer Erkenntnis
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	Lambda	Lambda Network Activity Monitoring	Mittel
UnauthorizedAccess:Lambda/TorClient	Lambda	Lambda Network Activity Monitoring	Hoch
UnauthorizedAccess:Lambda/TorRelay	Lambda	Lambda Network Activity Monitoring	Hoch
Execution:Container/MaliciousFile	Behälter	EBS-Malware-Schutz	Variiert je nach erkannter Bedrohung
Execution:Container/SuspiciousFile	Behälter	EBS-Malware-Schutz	Variiert je nach erkannter Bedrohung
Execution:EC2/MaliciousFile	Amazon EC2	EBS-Malware-Schutz	Variiert je nach erkannter Bedrohung
Execution:EC2/SuspiciousFile	Amazon EC2	EBS-Malware-Schutz	Variiert je nach erkannter Bedrohung
Execution:ECS/MaliciousFile	ECS	EBS-Malware-Schutz	Variiert je nach erkannter Bedrohung
Execution:ECS/SuspiciousFile	ECS	EBS-Malware-Schutz	Variiert je nach erkannter Bedrohung
Execution:Kubernetes/MaliciousFile	Kubernetes	EBS-Malware-Schutz	Variiert je nach erkannter Bedrohung
Execution:Kubernetes/SuspiciousFile	Kubernetes	EBS-Malware-Schutz	Variiert je nach erkannter Bedrohung
Execution:EC2/MaliciousFile!Snapshot	Amazon EBS	Malware Protection for Backup	Variiert je nach erkannter Bedrohung

Ergebnistyp	Ressourcentyp	Grundlegende Daten source/Feature	Der Schweregrad einer Erkenntnis
Execution:EC2/MaliciousFile!AMI	Amazon EC2	Malware Protection for Backup	Variiert je nach erkannter Bedrohung
Execution:EC2/MaliciousFile!RecoveryPoint	AWS Backup	Malware Protection for Backup	Variiert je nach erkannter Bedrohung
Execution:S3/MaliciousFile!RecoveryPoint	AWS Backup	Malware Protection for Backup	Variiert je nach erkannter Bedrohung
Object:S3/MaliciousFile	S3Objekt	Malware-Schutz für S3	Hoch
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	Unterstützte Amazon Aurora-, Amazon RDS- und Aurora Limitless-Datenbanken	RDS Login Activity Monitoring	Niedrig
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	Unterstützte Amazon Aurora-, Amazon RDS- und Aurora Limitless-Datenbanken	RDS Login Activity Monitoring	Hoch
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	Unterstützte Amazon Aurora-, Amazon RDS- und Aurora Limitless-Datenbanken	RDS Login Activity Monitoring	Variabel *

Ergebnistyp	Ressourcentyp	Grundlegende Daten source/Feature	Der Schweregrad einer Erkenntnis
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	Unterstützte Amazon Aurora-, Amazon RDS- und Aurora Limitless-Datenbanken	RDS Login Activity Monitoring	Mittel
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	Unterstützte Amazon Aurora-, Amazon RDS- und Aurora Limitless-Datenbanken	RDS Login Activity Monitoring	Hoch
CredentialAccess:RDS/TorIPCaller.FailedLogin	Unterstützte Amazon Aurora-, Amazon RDS- und Aurora Limitless-Datenbanken	RDS Login Activity Monitoring	Mittel
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	Unterstützte Amazon Aurora-, Amazon RDS- und Aurora Limitless-Datenbanken	RDS Login Activity Monitoring	Hoch
Discovery:RDS/MaliciousIPCaller	Unterstützte Amazon Aurora-, Amazon RDS- und Aurora Limitless-Datenbanken	RDS Login Activity Monitoring	Mittel
Discovery:RDS/TorIPCaller	Unterstützte Amazon Aurora-, Amazon RDS- und Aurora Limitless-Datenbanken	RDS Login Activity Monitoring	Mittel

Ergebnistyp	Ressourcentyp	Grundlegende Daten source/Feature	Der Schweregrad einer Erkenntnis
Discovery:S3/AnomalousBehavior	Amazon S3	CloudTrail Datenereignisse für S3	Niedrig
Discovery:S3/MaliciousIPCaller	Amazon S3	CloudTrail Datenereignisse für S3	Hoch
Discovery:S3/MaliciousIPCaller.Custom	Amazon S3	CloudTrail Datenereignisse für S3	Hoch
Discovery:S3/TorIPCaller	Amazon S3	CloudTrail Datenereignisse für S3	Mittel
Exfiltration:S3/AnomalousBehavior	Amazon S3	CloudTrail Datenereignisse für S3	Hoch
Exfiltration:S3/MaliciousIPCaller	Amazon S3	CloudTrail Datenereignisse für S3	Hoch
Impact:S3/AnomalousBehavior.Delete	Amazon S3	CloudTrail Datenereignisse für S3	Hoch
Impact:S3/AnomalousBehavior.Permission	Amazon S3	CloudTrail Datenereignisse für S3	Hoch
Impact:S3/AnomalousBehavior.Write	Amazon S3	CloudTrail Datenereignisse für S3	Mittel
Impact:S3/MaliciousIPCaller	Amazon S3	CloudTrail Datenereignisse für S3	Hoch
PenTest:S3/KaliLinux	Amazon S3	CloudTrail Datenereignisse für S3	Mittel
PenTest:S3/ParrotLinux	Amazon S3	CloudTrail Datenereignisse für S3	Mittel

Ergebnistyp	Ressourcentyp	Grundlegende Daten source/Feature	Der Schweregrad einer Erkenntnis
PenTest:S3/PentooLinux	Amazon S3	CloudTrail Datenereignisse für S3	Mittel
UnauthorizedAccess:S3/TorIPCaller	Amazon S3	CloudTrail Datenereignisse für S3	Hoch
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	Amazon S3	CloudTrail Datenereignisse für S3	Hoch
Backdoor:Runtime/C&CActivity.B	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Hoch
Backdoor:Runtime/C&CActivity.B!DNS	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Hoch
CryptoCurrency:Runtime/BitcoinTool.B	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Hoch
CryptoCurrency:Runtime/BitcoinTool.B!DNS	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Hoch
DefenseEvasion:Runtime/FilelessExecution	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Mittel
DefenseEvasion:Runtime/KernelModuleLoaded	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Daten source/Feature	Der Schweregrad einer Erkenntnis
DefenseEvasion:Runtime/SensitiveFileModified	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Mittel
DefenseEvasion:Runtime/ProcessInjection.Proc	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Hoch
DefenseEvasion:Runtime/ProcessInjection.Ptrace	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Mittel
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Hoch
DefenseEvasion:Runtime/PtraceAntiDebugging	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Niedrig
DefenseEvasion:Runtime/SuspiciousCommand	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Hoch
Discovery:Runtime/SuspiciousCommand	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Niedrig
Execution:Runtime/MaliciousFileExecuted	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Hoch
Execution:Runtime/MaliciousFileExecuted.Custom	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Daten source/Feature	Der Schweregrad einer Erkenntnis
Execution:Runtime/NewBinaryExecuted	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Mittel
Execution:Runtime/NewLibraryLoaded	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Mittel
Execution:Runtime/SuspiciousCommand	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Variable
Execution:Runtime/SuspiciousShellCreated	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Niedrig
Execution:Runtime/SuspiciousTool	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Variable
Execution:Runtime/ReverseShell	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Hoch
Impact:Runtime/AbusedDomainRequest.Reputation	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Mittel
Impact:Runtime/BitcoinDomainRequest.Reputation	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Hoch
Impact:Runtime/CryptoMinerExecuted	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Daten source/Feature	Der Schweregrad einer Erkenntnis
Impact:Runtime/MaliciousDomainRequest.Reputation	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Mittel
Impact:Runtime/SuspiciousDomainRequest.Reputation	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Niedrig
Persistence:Runtime/SuspiciousCommand	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Mittel
Persistence:Runtime/SensitiveFileModified	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Mittel
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Hoch
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Mittel
PrivilegeEscalation:Runtime/DockerSocketAccessed	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Mittel
PrivilegeEscalation:Runtime/ElevationToRoot	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Mittel
PrivilegeEscalation:Runtime/RuncContainerEscape	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Daten source/Feature	Der Schweregrad einer Erkenntnis
PrivilegeEscalation:Runtime/SuspiciousCommand	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Mittel
PrivilegeEscalation:Runtime/SensitiveFileModified	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Mittel
PrivilegeEscalation:Runtime/UserfaultfdUsage	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Mittel
Trojan:Runtime/BlackholeTraffic	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Mittel
Trojan:Runtime/BlackholeTraffic! DNS	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Mittel
Trojan:Runtime/DropPoint	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Mittel
Trojan:Runtime/DGADomainRequest.C! DNS	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Hoch
Trojan:Runtime/DriveBySourceTraffic! DNS	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Hoch
Trojan:Runtime/DropPoint! DNS	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Mittel

Ergebnistyp	Ressourcentyp	Grundlegende Daten source/Feature	Der Schweregrad einer Erkenntnis
Trojan:Runtime/PhishingDomainRequest! DNS	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Hoch
UnauthorizedAccess:Runtime/MetadataDNSRebind	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Hoch
UnauthorizedAccess:Runtime/TorClient	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Hoch
UnauthorizedAccess:Runtime/TorRelay	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeitüberwachung	Hoch

GuardDuty Amazon-Ergebnisse verstehen und generieren

Ein GuardDuty Ergebnis steht für ein potenzielles Sicherheitsproblem AWS-Konten, das in Workloads und Daten erkannt wurde. GuardDuty generiert ein Ergebnis, wenn unerwartete und potenziell bösartige Aktivitäten in Ihrer AWS Umgebung erkannt werden.

Sie können Ihre GuardDuty Ergebnisse auf der Seite „Ergebnisse“ in der GuardDuty Konsole oder mithilfe der AWS CLI oder API-Operationen anzeigen und verwalten. Informationen darüber, wie Sie GuardDuty Ergebnisse verwalten können, finden Sie unterVerwaltung der GuardDuty Amazon-Ergebnisse.

Themen:

GuardDuty Format finden

Machen Sie sich mit dem Format der GuardDuty Suche nach Typen und den verschiedenen Zwecken vertraut, mit denen die Bedrohungen GuardDuty verfolgt werden.

Beispielerkenntnisse

Generieren Sie Beispielergebnisse in der GuardDuty Konsole oder mithilfe von GuardDuty APIs oder AWS CLI Befehlen. Die generierten Stichprobenergebnisse enthalten fiktive Details, damit Sie die mit den einzelnen GuardDuty Ergebnissen verbundenen Befunddetails besser verstehen können. Diese Ergebnisse sind mit einem Präfix [SAMPLE] gekennzeichnet.

GuardDuty Testergebnisse in speziellen Konten

Sie können bestimmte GuardDuty Ergebnisse in Ihrer Umgebung testen. Führen Sie `guardduty-tester` das Skript in einer dedizierten Nicht-Produktionsumgebung AWS-Konto aus. GuardDuty Um die Ergebnisse zu erkennen und zu simulieren, werden bestimmte Ressourcen in Ihrer Umgebung bereitgestellt. Diese Erfahrung unterscheidet sich von der Generierung von Stichprobenergebnissen.

Generierte Ergebnisse in der GuardDuty Konsole anzeigen

Erfahren Sie, wie Sie die generierten Ergebnisse in der GuardDuty Konsole überprüfen können.

Schweregrad der Ergebnisse GuardDuty

Jedem GuardDuty Befund ist ein Schweregrad zugeordnet, der das potenzielle Risiko in Ihrer AWS Umgebung widerspiegelt. In diesem Abschnitt wird erklärt, was die einzelnen Schweregrade bedeuten.

Erkenntnisdetails

Erfahren Sie mehr über die Details zu den GuardDuty Ergebnissen, die in Ihrem Konto generiert werden. Dieses Thema enthält die Einzelheiten zur grundlegenden Bedrohungserkennung, zur erweiterten Bedrohungserkennung und zu speziellen Schutzplänen unter GuardDuty.

GuardDuty Aggregation finden

Erfahren Sie, wie GuardDuty mit mehreren Vorkommen desselben Ergebnistyps umgegangen wird. Durch die Aggregation erkannter derselben Ergebnisarten wird der ursprüngliche Ergebnistyp mit den neuesten Details GuardDuty aktualisiert.

GuardDuty Typen finden

In diesem Abschnitt wird das GuardDuty Finden von Typen anhand des zugehörigen Grundlegende Datenquellen oder beschrieben. Zugeordnete Funktion GuardDuty Um mehr über die einzelnen Befundarten zu erfahren, wählen Sie das jeweilige Ergebnis aus, um weitere Informationen zu erhalten, z. B. eine Beschreibung und mögliche Schritte zur Behebung des Ergebnisses.

GuardDuty Format finden

Wenn verdächtiges oder unerwartetes Verhalten in Ihrer AWS Umgebung GuardDuty erkannt wird, wird ein Befund generiert. Ein Befund ist eine Benachrichtigung, die Einzelheiten zu einem potenziellen Sicherheitsproblem enthält, das GuardDuty entdeckt wurde. Sie Generierte Ergebnisse in der GuardDuty Konsole anzeigen enthalten Informationen darüber, was passiert ist, welche AWS Ressourcen an der verdächtigen Aktivität beteiligt waren, wann diese Aktivität stattgefunden hat, sowie zugehörige Informationen, die Ihnen helfen können, die Ursache zu verstehen.

Eine der wichtigsten Informationen in den Ergebnisdetails ist der Ergebnistyp. Der Zweck des Ergebnistyps ist eine kurze und dennoch aussagekräftige Beschreibung des potenziellen Sicherheitsrisikos. Anhand des Suchtyps werden Sie beispielsweise schnell darüber informiert, dass irgendwo in Ihrer AWS Umgebung eine EC2-Instance über einen ungeschützten Port verfügt, den ein potenzieller Angreifer GuardDuty Recon:EC2/PortProbeUnprotectedPortausfindig macht.

GuardDuty verwendet das folgende Format für die Benennung der verschiedenen Arten von Ergebnissen, die es generiert:

ThreatPurpose:ResourceTypeAffected/ThreatFamilyName.DetectionMechanism! Artifact

Jeder Teil dieses Formats steht für einen Aspekt eines Erkenntnistyps. Für diese Aspekte gibt es die folgenden Erklärungen:

- ThreatPurpose- beschreibt den Hauptzweck einer Bedrohung, einen Angriffstyp oder eine Phase eines potenziellen Angriffs. Im folgenden Abschnitt finden Sie eine vollständige Liste der GuardDuty Bedrohungszwecke.
- ResourceTypeAffected— beschreibt, welcher AWS Ressourcentyp in diesem Ergebnis als potenzielles Ziel eines Widersachers identifiziert wurde. GuardDuty Kann derzeit Ergebnisse für die Ressourcentypen generieren, die in der aufgeführt sind. GuardDuty Typen von aktiven Ergebnissen
- ThreatFamilyName- beschreibt die allgemeine Bedrohung oder potenzielle bösartige Aktivität, die erkannt GuardDuty wird. Ein Wert von NetworkPortUnusualgibt beispielsweise an, dass eine im GuardDuty Ergebnis identifizierte EC2-Instance keine vorherige Kommunikationshistorie an einem bestimmten Remote-Port hatte, der auch im Ergebnis identifiziert wurde.
- DetectionMechanism- beschreibt die Methode, mit der der Befund GuardDuty erkannt wurde. Dies kann verwendet werden, um auf eine Variation eines gemeinsamen Befundtyps oder auf ein Ergebnis hinzuweisen, GuardDuty bei dem ein bestimmter Erkennungsmechanismus verwendet wurde. Backdoor:EC2/DenialOfService.TcpZeigt beispielsweise an, dass ein Denial of Service (DoS) über TCP erkannt wurde. Die UDP-Variante ist Backdoor:EC2/DenialOfService.Udp.

  Der Wert .Custom gibt an, dass das Ergebnis anhand Ihrer benutzerdefinierten Bedrohungslisten GuardDuty erkannt wurde. Weitere Informationen finden Sie unter Entitätslisten und IP-Adresslisten.

  Der Wert .Reputation gibt an, dass das Ergebnis anhand eines Domain-Reputations-Score-Modells GuardDuty erkannt wurde. Weitere Informationen finden Sie unter So können Sie AWS die größten Sicherheitsbedrohungen der Cloud aufspüren und sie abwehren.
- Artefakt – Eine Beschreibung einer bestimmten Ressource eines Tools, das beim Angriff verwendet wird. Beispielsweise weist DNS im Findingtyp CryptoCurrency:EC2/BitcoinTool.B!DNS darauf hin, dass eine Amazon EC2 EC2-Instance mit einer bekannten Bitcoin-related Domain kommuniziert.

> **Note**
>
> Artifact ist optional und möglicherweise nicht für alle GuardDuty Fundtypen verfügbar.

Bedrohungszwecke

In GuardDuty einer Bedrohung beschreibt Zweck den Hauptzweck einer Bedrohung, einen Angriffstyp oder eine Phase eines potenziellen Angriffs. Beispielsweise deuten einige Bedrohungszwecke, wie Backdoor, auf einen Typ von Angriff hin. Einige Bedrohungszwecke, wie etwa Impact, stimmen jedoch mit den Taktiken von MITRE ATT&CK überein. Die MITRE-ATT&CK-Taktiken deuten auf verschiedene Phasen im Angriffszyklus eines Gegners hin. In der aktuellen Version von GuardDuty ThreatPurpose kann es die folgenden Werte haben:

Backdoor

Dieser Wert gibt an, dass ein Angreifer eine Ressource kompromittiert und die AWS Ressource so verändert hat, dass er seinen Home-Command-and-Control-Server (C&C) kontaktieren kann, um weitere Anweisungen für böswillige Aktivitäten zu erhalten.

Behavior

Dieser Wert gibt an, GuardDuty dass Aktivitäten oder Aktivitätsmuster erkannt wurden, die sich von der festgelegten Ausgangsbasis für die beteiligten Ressourcen unterscheiden. AWS

CredentialAccess

Dieser Wert gibt an, dass GuardDuty Aktivitätsmuster erkannt wurden, anhand derer ein Angreifer Anmeldeinformationen wie Passwörter, Benutzernamen und Zugriffsschlüssel aus Ihrer Umgebung stehlen kann. Dieser Bedrohungszweck basiert auf der MITRE-ATT&CK-Taktiken.

Kryptowährung

Dieser Wert gibt an, dass erkannt GuardDuty wurde, dass eine AWS Ressource in Ihrer Umgebung Software hostet, die mit Kryptowährungen verknüpft ist (z. B. Bitcoin).

DefenseEvasion

Dieser Wert gibt an, GuardDuty dass Aktivitäten oder Aktivitätsmuster erkannt wurden, anhand derer ein Angreifer beim Eindringen in Ihre Umgebung möglicherweise nicht entdeckt wird. Dieser Bedrohungszweck basiert auf den MITRE-ATT&CK-Taktiken

Erkennung

Dieser Wert gibt an, GuardDuty dass Aktivitäten oder Aktivitätsmuster erkannt wurden, anhand derer ein Angreifer sein Wissen über Ihre Systeme und internen Netzwerke erweitern kann. Dieser Bedrohungszweck basiert auf der MITRE-ATT&CK-Taktiken.

Ausführung

Dieser Wert gibt an, dass erkannt GuardDuty wurde, dass ein Angreifer möglicherweise versucht, bösartigen Code auszuführen, um die AWS Umgebung zu erkunden oder Daten zu stehlen. Dieser Bedrohungszweck basiert auf der MITRE-ATT&CK-Taktiken.

Exfiltration

Dieser Wert gibt an, GuardDuty dass Aktivitäten oder Aktivitätsmuster erkannt wurden, die ein Angreifer verwenden könnte, wenn er versucht, Daten aus Ihrer Umgebung zu stehlen. Dieser Bedrohungszweck basiert auf der MITRE-ATT&CK-Taktiken.

Auswirkung

Dieser Wert gibt an, GuardDuty dass Aktivitäten oder Aktivitätsmuster erkannt wurden, die darauf hindeuten, dass ein Angreifer versucht, Ihre Systeme und Daten zu manipulieren, zu unterbrechen oder zu zerstören. Dieser Bedrohungszweck basiert auf der MITRE-ATT&CK-Taktiken.

InitialAccess

Dieser Wert wird üblicherweise mit der ersten Zugriffsphase eines Angriffs in Verbindung gebracht, wenn ein Angreifer versucht, Zugriff auf Ihre Umgebung zu erhalten. Dieser Bedrohungszweck basiert auf der MITRE-ATT&CK-Taktiken.

Penetrationstest

Manchmal führen Besitzer von AWS Ressourcen oder ihre autorisierten Vertreter bewusst Tests mit AWS Anwendungen durch, um Sicherheitslücken zu finden, z. B. offene Sicherheitsgruppen oder zu freizügige Zugriffsschlüssel. Bei diesen Penetrationstests wird versucht, gefährdete Ressourcen zu erkennen und zu sperren, bevor sie von Angreifern entdeckt werden. Einige der von autorisierten Penetrationstestern verwendeten Tools sind jedoch kostenlos verfügbar und können daher auch von nicht autorisierten Benutzern oder Angreifern verwendet werden, um Analysetests durchzuführen. Obwohl der wahre Zweck einer solchen Aktivität nicht identifiziert werden GuardDuty kann, gibt der Pentest-Wert an, dass eine solche Aktivität erkannt GuardDuty wird, dass sie der Aktivität ähnelt, die von bekannten Pen-Testing-Tools generiert wird, und dass dies auf böswillige Tests in Ihrem Netzwerk hinweisen könnte.

Persistenz

Dieser Wert gibt an, GuardDuty dass Aktivitäten oder Aktivitätsmuster erkannt wurden, anhand derer ein Angreifer versuchen könnte, den Zugriff auf Ihre Systeme aufrechtzuerhalten, auch wenn der ursprüngliche Zugriffsweg unterbrochen ist. Dies könnte beispielsweise das

Erstellen eines neuen IAM-Benutzers beinhalten, nachdem er über die kompromittierten Anmeldeinformationen eines vorhandenen Benutzers Zugriff erhalten hat. Wenn die Anmeldeinformationen des vorhandenen Benutzers gelöscht werden, behält der Angreifer den Zugriff auf den neuen Benutzer, der beim ursprünglichen Ereignis nicht erkannt wurde. Dieser Bedrohungszweck basiert auf der MITRE-ATT&CK-Taktiken.

Richtlinie

Dieser Wert weist darauf hin, AWS-Konto dass Ihr Verhalten gegen die empfohlenen bewährten Sicherheitsmethoden verstößt. Zum Beispiel unbeabsichtigte Änderungen von Berechtigungsrichtlinien in Bezug auf Ihre AWS Ressourcen oder Ihre Umgebung und die Verwendung von privilegierten Konten, die kaum oder gar nicht genutzt werden sollten.

PrivilegeEscalation

Dieser Wert informiert Sie darüber, dass der betroffene Prinzipal in Ihrer AWS -Umgebung ein Verhalten an den Tag legt, das ein Angreifer nutzen könnte, um sich Zugriff auf Ihr Netzwerk auf höherer Ebene zu verschaffen. Dieser Bedrohungszweck basiert auf der MITRE-ATT&CK-Taktiken.

Recon

Dieser Wert gibt an, GuardDuty dass Aktivitäten oder Aktivitätsmuster erkannt wurden, anhand derer ein Angreifer Ihre Umgebung auskundschaften kann, um zu ermitteln, wie er seinen Zugriff erweitern oder Ihre Ressourcen nutzen kann. Diese Aktivität kann beispielsweise das Aufspüren von Sicherheitslücken in Ihrer AWS Umgebung umfassen, indem Sie unter anderem Ports sondieren, API-Aufrufe tätigen, Benutzer auflisten und Datenbanktabellen auflisten.

Stealth

Dieser Wert gibt an, dass ein Angreifer aktiv versucht, seine Aktionen zu verbergen. Beispielsweise könnten sie einen anonymisierenden Proxyserver verwenden, was es extrem schwierig macht, die wahre Art der Aktivität einzuschätzen.

Trojan

Dieser Wert gibt an, dass der Angriff über Trojaner-Programme erfolgt, die im Hintergrund schädliche Aktivitäten durchführen. Es kann vorkommen, dass diese Software das Erscheinungsbild eines seriösen Programms annimmt. Es kann vorkommen, dass Benutzer diese Software versehentlich ausführen. Die Software kann auch automatisch durch Ausnutzung einer Schwachstelle ausgeführt werden.

UnauthorizedAccess

Dieser Wert gibt an, dass GuardDuty eine verdächtige Aktivität oder ein verdächtiges Aktivitätsmuster durch eine nicht autorisierte Person erkannt wird.

GuardDuty Scan-Engine zur Malware-Erkennung

Amazon GuardDuty hat eine intern entwickelte und verwaltete Scan-Engine und einen Drittanbieter. Beide verwenden Kompromittierungsindikatoren (IoCs), die aus verschiedenen internen Feeds stammen und Aufschluss über verschiedene Arten von Schadsoftware geben, auf die möglicherweise zugegriffen werden kann AWS. GuardDuty verfügt außerdem über Erkennungsdefinitionen, die auf YARA-Regeln basieren, die von unseren Sicherheitsingenieuren hinzugefügt wurden, sowie Erkennungen, die auf heuristischen Modellen und Modellen für maschinelles Lernen (ML) basieren. Beim Scannen von Amazon S3 S3-Objekten liefert GuardDuty Malware Protection konsistente Ergebnisse, wenn dasselbe Objekt mehrmals mit denselben Scandefinitionen und Engines gescannt wird. Signature-based Die Erkennung umfasst nicht nur den Abgleich von Bytes, sondern auch einen Codeausschnitt, der potenziell komplex ist, und der Scanner kann Inhalte analysieren und Entscheidungen treffen.

Die Malware-Scan-Engine führt keine Live-Verhaltensanalyse durch, bei der die Malware-Detonation die Probe überwacht, während sie in einem realen System ausgeführt wird. Die GuardDuty Lösung besteht in erster Linie in einer dateibasierten Erkennung. GuardDuty Bietet eine agentenbasierte Lösung zur Erkennung dateiloser Malware, z. B. Laufzeitüberwachung für Amazon EKS, Amazon EC2 und Amazon ECS (einschließlich). AWS Fargate

Die verwendeten Scan-Engines sind in der Lage, verschiedene Arten von Malware wie Cryptominer, Ransomware und Webshells zu erkennen, da es keine Einschränkungen hinsichtlich der Dateiformate gibt, mit denen nach Malware GuardDuty gescannt wird. Die vollständig verwaltete GuardDuty Scan-Engine aktualisiert die Liste der Malware-Signaturen kontinuierlich alle 15 Minuten.

Die Scan-Engine ist Teil eines GuardDuty Threat Intelligence-Systems, das eine interne Komponente zur Detonation von Malware verwendet. Dadurch werden neue Bedrohungsinformationen generiert, indem unabhängig voneinander Malware und harmlose Proben aus verschiedenen Quellen gesammelt werden. Der IoC-Typ Datei-Hash aus dem Threat Intelligence System wird außerdem in die Malware-Scan-Engine eingespeist, um Malware auf der Grundlage bekannter bösartiger Datei-Hashes zu erkennen.

Generierung von Stichprobenbefunden in GuardDuty

Amazon GuardDuty hilft Ihnen bei der Generierung von Stichprobenergebnissen, um die verschiedenen Arten von Ergebnissen, die generiert werden können, zu visualisieren und zu verstehen. Wenn Sie Stichprobenergebnisse generieren, GuardDuty füllt Ihre aktuelle Ergebnisliste mit einer Stichprobe für jeden unterstützten Ergebnistyp auf, einschließlich der Arten von Angriffssequenzen.

Bei den generierten Beispielen handelt es sich um Näherungen, die mit Platzhalterwerten gefüllt sind. Diese Beispiele sehen möglicherweise anders aus als die tatsächlichen Ergebnisse für Ihre Umgebung, aber Sie können sie verwenden, um verschiedene Konfigurationen zu testen GuardDuty, z. B. auf Ihre EventBridge Ereignisse oder Filter. Eine Liste der verfügbaren Werte für die Suche nach Typen finden Sie in der GuardDuty Typen finden Tabelle.

Generierung von Beispielergebnissen über die GuardDuty Konsole oder API

Wählen Sie Ihre bevorzugte Zugriffsmethode, um Beispiel-Erkenntnisse zu generieren.

> **Note**
>
> Die GuardDuty Konsole hilft Ihnen bei der Generierung eines Ergebnisses für jeden Ergebnistyp. Um einen oder mehrere bestimmte Ergebnisarten zu generieren, führen Sie die zugehörigen API/CLI Schritte aus.

Console

Gehen Sie wie folgt vor, um Beispielergebnisse zu erzeugen. Bei diesem Verfahren wird für jeden Befundtyp ein GuardDuty Stichprobenergebnis generiert.

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Klicken Sie auf der Seite Settings unter Sample findings auf Generate sample findings.
4. Wählen Sie im Navigationsbereich Findings aus. Die Beispiel-Erkenntnisse werden auf der Seite Aktuelle Erkenntnisse mit dem Präfix [SAMPLE] angezeigt.

API/CLI

Sie können über die CreateSampleFindings API ein einzelnes Stichprobenergebnis generieren, GuardDuty das einem der Suchtypen entspricht. Die verfügbaren Werte für die Suchtypen sind in der GuardDuty Typen finden Tabelle aufgeführt.

Dies ist nützlich, um CloudWatch Event-Regeln oder die Automatisierung auf der Grundlage von Ergebnissen zu testen. Das folgende Beispiel zeigt, wie Sie ein einzelnes Beispiel-Erkenntnis des `Backdoor:EC2/DenialOfService.Tcp`-Typs mithilfe der AWS CLI generieren können.

Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

```
aws guardduty create-sample-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --finding-types Backdoor:EC2/DenialOfService.Tcp
```

Der Titel der mit diesen Methoden generierten Beispiel-Erkenntnisse beginnt in der Konsole immer mit [SAMPLE]. Beispiel-Erkenntnisse haben im Abschnitt additionalInfo der JSON-Erkenntnis-Details den Wert von `"sample": true`.

Informationen zu den mit den generierten Ergebnissen verknüpften Befunddetails, z. B. dem Schweregrad des Fundes und der potenziell gefährdeten Ressource, finden Sie unter Schweregrad der Ergebnisse GuardDuty undErkenntnisdetails.

Informationen zum Generieren einiger allgemeiner Ergebnisse auf der Grundlage einer simulierten Aktivität in einer dedizierten und isolierten Umgebung AWS-Konto innerhalb Ihrer Umgebung finden Sie unter. GuardDuty Testergebnisse in speziellen Konten

GuardDuty Testergebnisse in speziellen Konten

Verwenden Sie dieses Dokument, um ein Tester-Skript auszuführen, das GuardDuty Ergebnisse anhand von Testressourcen generiert, die in Ihrem bereitgestellt werden AWS-Konto. Sie können diese Schritte ausführen, wenn Sie mehr über bestimmte GuardDuty Ergebnisarten und darüber erfahren möchten, wie die Ergebnisdetails für die tatsächlichen Ressourcen in Ihrem Konto aussehen. Diese Erfahrung unterscheidet sich von der GenerierungBeispielerkenntnisse. Weitere Informationen zu den Erfahrungen beim Testen von GuardDuty Ergebnissen finden Sie unterÜberlegungen.

Inhalt

- Überlegungen
- GuardDuty Ergebnisse, die das Tester-Skript generieren kann
- Schritt 1 — Voraussetzungen
- Schritt 2 — Ressourcen bereitstellen AWS
- Schritt 3 — Führen Sie Tester-Skripte aus
- Schritt 4 — Testressourcen AWS bereinigen
- Behebung häufiger Probleme

Überlegungen

Bevor Sie fortfahren, sollten Sie die folgenden Überlegungen berücksichtigen:

- GuardDuty empfiehlt, den Tester an einem speziellen Ort außerhalb der AWS-Konto Produktionsumgebung einzusetzen. Dieser Ansatz stellt sicher, dass Sie die vom Tester generierten GuardDuty Ergebnisse korrekt identifizieren können. Darüber hinaus stellt der GuardDuty Tester eine Vielzahl von Ressourcen bereit, für die möglicherweise IAM-Berechtigungen erforderlich sind, die über die Rechte anderer Konten hinausgehen. Durch die Verwendung eines dedizierten Kontos wird sichergestellt, dass der Umfang der Berechtigungen ordnungsgemäß und mit einer klaren Kontogrenze festgelegt werden kann.
- Das Tester-Skript generiert über 100 GuardDuty Ergebnisse mit unterschiedlichen AWS Ressourcenkombinationen. Derzeit beinhaltet dies nicht alle. GuardDuty Typen finden Eine Liste der Suchtypen, die Sie mit diesem Tester-Skript generieren können, finden Sie unter. GuardDuty Ergebnisse, die das Tester-Skript generieren kann

  > **Hinweis**
  >
  > Um die Suchtypen der Angriffssequenz zu visualisieren, generiert das Tester-Skript nur AttackSequence:EKS/CompromisedCluster undAttackSequence:S3/CompromisedData. Zur Visualisierung und zum AttackSequence:IAM/CompromisedCredentials besseren Verständnis können Sie Beispielerkenntnisse in Ihrem Konto generieren.

- Damit der GuardDuty Tester wie erwartet funktioniert, GuardDuty muss er in dem Konto aktiviert sein, in dem die Tester-Ressourcen bereitgestellt werden. Abhängig von den Tests, die ausgeführt werden, bewertet der Tester, ob die entsprechenden GuardDuty Schutzpläne aktiviert sind

oder nicht. Für jeden Schutzplan, der nicht aktiviert ist, bittet GuardDuty er um Erlaubnis, die erforderlichen Schutzpläne so lange zu aktivieren, GuardDuty bis die Tests durchgeführt werden können, die zu Ergebnissen führen. GuardDuty Wird den Schutzplan später deaktivieren, sobald die Tests abgeschlossen sind.

GuardDuty Zum ersten Mal aktivieren

Wenn GuardDuty es in Ihrem speziellen Konto zum ersten Mal in einer bestimmten Region aktiviert wird, wird Ihr Konto automatisch für eine kostenlose 30-Tage-Testversion registriert.

GuardDuty bietet optionale Schutzpläne. Zum Zeitpunkt der Aktivierung GuardDuty werden auch bestimmte Schutzpläne aktiviert und sind in der kostenlosen GuardDuty 30-Tage-Testversion enthalten. Weitere Informationen finden Sie unter Nutzen Sie die kostenlose GuardDuty 30-Tage-Testversion.

GuardDuty ist in Ihrem Konto bereits aktiviert, bevor Sie das Tester-Skript ausführen

Wenn GuardDuty es bereits aktiviert ist, überprüft das Tester-Skript anhand der Parameter den Konfigurationsstatus bestimmter Schutzpläne und anderer Einstellungen auf Kontoebene, die zur Generierung der Ergebnisse erforderlich sind.

Durch die Ausführung dieses Testerskripts können bestimmte Schutzpläne in Ihrem speziellen Konto in einer Region zum ersten Mal aktiviert werden. Dadurch wird die kostenlose 30-Tage-Testversion für diesen Schutzplan gestartet. Informationen zu den kostenlosen Testversionen der einzelnen Schutzpläne finden Sie unterNutzen Sie die kostenlose GuardDuty 30-Tage-Testversion.

- Solange die GuardDuty Tester-Infrastruktur bereitgestellt ist, können Sie gelegentlich UnauthorizedAccess:EC2/TorClient Ergebnisse aus der PenTest Instanz erhalten.

GuardDuty Ergebnisse, die das Tester-Skript generieren kann

Derzeit generiert das Tester-Skript die folgenden Findtypen, die sich auf Amazon EC2-, Amazon EKS-, Amazon S3-, IAM- und EKS-Audit-Logs beziehen:

- AttackSequence:EKS/CompromisedCluster
- AttackSequence:S3/CompromisedData
- Backdoor:EC2/C&CActivity.B!DNS
- Backdoor:EC2/DenialOfService.Dns
- Backdoor:EC2/DenialOfService.Udp

- CryptoCurrency:EC2/BitcoinTool.B!DNS
- Impact:EC2/AbusedDomainRequest.Reputation
- Impact:EC2/BitcoinDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Reputation
- Impact:EC2/SuspiciousDomainRequest.Reputation
- Recon:EC2/Portscan
- Trojan:EC2/BlackholeTraffic!DNS
- Trojan:EC2/DGADomainRequest.C!DNS
- Trojan:EC2/DNSDataExfiltration
- Trojan:EC2/DriveBySourceTraffic!DNS
- Trojan:EC2/DropPoint!DNS
- Trojan:EC2/PhishingDomainRequest!DNS
- UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
- UnauthorizedAccess:EC2/RDPBruteForce
- UnauthorizedAccess:EC2/SSHBruteForce
- PenTest:IAMUser/KaliLinux
- Recon:IAMUser/MaliciousIPCaller.Custom
- Recon:IAMUser/TorIPCaller
- Stealth:IAMUser/CloudTrailLoggingDisabled
- Stealth:IAMUser/PasswordPolicyChange
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
- UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom
- UnauthorizedAccess:IAMUser/TorIPCaller
- Discovery:Kubernetes/MaliciousIPCaller.Custom
- Discovery:Kubernetes/SuccessfulAnonymousAccess
- Discovery:Kubernetes/TorIPCaller
- Execution:Kubernetes/ExecInKubeSystemPod
- Impact:Kubernetes/MaliciousIPCaller.Custom
- Persistence:Kubernetes/ContainerWithSensitiveMount
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount

- Policy:Kubernetes/AnonymousAccessGranted
- PrivilegeEscalation:Kubernetes/PrivilegedContainer
- UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom
- Discovery:S3/MaliciousIPCaller.Custom
- Discovery:S3/TorIPCaller
- PenTest:S3/KaliLinux
- Policy:S3/AccountBlockPublicAccessDisabled
- Policy:S3/BucketAnonymousAccessGranted
- Policy:S3/BucketBlockPublicAccessDisabled
- Policy:S3/BucketPublicAccessGranted
- Stealth:S3/ServerAccessLoggingDisabled
- UnauthorizedAccess:S3/MaliciousIPCaller.Custom
- UnauthorizedAccess:S3/TorIPCaller
- Backdoor:Runtime/C&CActivity.B! DNS
- CryptoCurrency:Runtime/BitcoinTool.B! DNS
- DefenseEvasion:Runtime/ProcessInjection.Ptrace
- DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite
- Execution:Runtime/ReverseShell
- Impact:Runtime/AbusedDomainRequest.Reputation
- Impact:Runtime/BitcoinDomainRequest.Reputation
- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation
- PrivilegeEscalation:Runtime/ContainerMountsHostDirectory
- PrivilegeEscalation:Runtime/DockerSocketAccessed
- Trojan:Runtime/BlackholeTraffic! DNS
- Trojan:Runtime/DGADomainRequest.C! DNS
- Trojan:Runtime/DriveBySourceTraffic! DNS
- Trojan:Runtime/DropPoint! DNS
- Trojan:Runtime/PhishingDomainRequest! DNS

Schritt 1 — Voraussetzungen

Um Ihre Testumgebung vorzubereiten, benötigen Sie die folgenden Elemente:

- Git — Installieren Sie das Git-Befehlszeilentool basierend auf dem von Ihnen verwendeten Betriebssystem.

  Dies ist erforderlich, um das `amazon-guardduty-tester`Repository zu klonen.
- AWS Command Line Interface— Ein Open-Source-Tool, mit dem Sie mithilfe AWS-Services von Befehlen in Ihrer Befehlszeilen-Shell interagieren können. Weitere Informationen finden Sie unter Erste Schritte mit AWS CLI im AWS Command Line Interface Benutzerhandbuch.
- AWS Systems Manager— Um Session Manager-Sitzungen mit Ihren verwalteten Knoten zu initiieren, müssen AWS CLI Sie das Session Manager-Plug-In auf Ihrem lokalen Computer installieren. Weitere Informationen finden Sie unter Installieren des Session Manager-Plug-ins für AWS CLI im AWS Systems Manager Benutzerhandbuch.
- Node Package Manager (NPM) — Installieren Sie NPM, um alle Abhängigkeiten zu installieren.
- Docker — Sie müssen Docker installiert haben. Installationsanweisungen finden Sie auf der Docker-Website.

  Um zu überprüfen, ob Docker installiert wurde, führen Sie den folgenden Befehl aus und vergewissern Sie sich, dass eine Ausgabe vorliegt, die der folgenden Ausgabe ähnelt:

  ```
  $ docker --version
  Docker version 19.03.1
  ```
- Abonnieren Sie das Kali Linux-Image im. AWS Marketplace

Schritt 2 — Ressourcen bereitstellen AWS

Dieser Abschnitt enthält eine Liste der wichtigsten Konzepte und der Schritte zur Bereitstellung bestimmter AWS Ressourcen in Ihrem speziellen Konto.

Konzepte

Die folgende Liste enthält wichtige Konzepte zu den Befehlen, mit denen Sie die Ressourcen bereitstellen können:

- AWS Cloud Development Kit (AWS CDK)— CDK ist ein Open-Source-Framework für die Softwareentwicklung, mit dem Cloud-Infrastruktur im Code definiert und bereitgestellt werden kann. CloudFormation CDK unterstützt eine Reihe von Programmiersprachen, um wiederverwendbare Cloud-Komponenten, sogenannte Konstrukte, zu definieren. Sie können diese zu Stacks und Apps zusammenstellen. Anschließend können Sie Ihre CDK-Anwendungen bereitstellen, CloudFormation um Ihre Ressourcen bereitzustellen oder zu aktualisieren. Weitere Informationen finden Sie unter Was ist der AWS CDK? im AWS Cloud Development Kit (AWS CDK) Entwicklerhandbuch.
- Bootstrapping — Dies ist der Prozess, bei dem Ihre AWS Umgebung für die Verwendung mit vorbereitet wird. AWS CDK Bevor Sie einen CDK-Stack in einer AWS Umgebung bereitstellen, muss die Umgebung zunächst gebootet werden. Dieser Prozess der Bereitstellung bestimmter AWS Ressourcen in Ihrer Umgebung, die von verwendet werden, AWS CDK ist Teil der Schritte, die Sie im nächsten Abschnitt ausführen werden -. Schritte zur Bereitstellung von Ressourcen AWS

  Weitere Informationen zur Funktionsweise von Bootstrapping finden Sie unter Bootstrapping im Entwicklerhandbuch.AWS Cloud Development Kit (AWS CDK)

Schritte zur Bereitstellung von Ressourcen AWS

Führen Sie die folgenden Schritte aus, um mit der Bereitstellung der Ressourcen zu beginnen:

1. Richten Sie Ihr AWS CLI Standardkonto und Ihre Region ein, sofern die Regionsvariablen für das Konto nicht manuell in der `bin/cdk-gd-tester.ts` Datei festgelegt wurden. Weitere Informationen finden Sie im AWS Cloud Development Kit (AWS CDK) Entwicklerhandbuch unter Umgebungen.
2. Führen Sie die folgenden Befehle aus, um die Ressourcen bereitzustellen:

   ```
   git clone https://github.com/awslabs/amazon-guardduty-tester && cd amazon-guardduty-tester
   npm install
   cdk bootstrap
   cdk deploy
   ```

   Der letzte Befehl (`cdk deploy`) erstellt in Ihrem Namen einen CloudFormation Stack. Der Name dieses Stacks ist GuardDutyTesterStack.

GuardDuty Erstellt im Rahmen dieses Skripts neue Ressourcen, um GuardDuty Ergebnisse in Ihrem Konto zu generieren. Außerdem wird den Amazon EC2 EC2-Instances das folgende Tag-Schlüssel:Wert-Paar hinzugefügt:

```
CreatedBy:GuardDuty Test Script
```

Zu den Amazon EC2 EC2-Instances gehören auch die EC2-Instances, die EKS-Knoten und ECS-Cluster hosten.

> **Instance-Typen**
>
> GuardDuty wurde für die Verwendung kostengünstiger Instance-Typen entwickelt, die die Mindestleistung bieten, die für die erfolgreiche Durchführung von Tests erforderlich ist. Aufgrund der vCPU-Anforderungen, die die Amazon EKS-Knotengruppe benötigt`t3.medium`, und aufgrund der erhöhten Netzwerkkapazität, die für die DenialOfService Suche nach Tests erforderlich ist, benötigt `m6i.large` der Treiberknoten. GuardDuty Verwendet für alle anderen Tests den `t3.micro` Instance-Typ. Weitere Informationen zu Instance-Typen finden Sie unter Verfügbare Größen im Amazon EC2 Instances Types Guide.

Schritt 3 — Führen Sie Tester-Skripte aus

Dies ist ein zweistufiger Prozess, bei dem Sie zuerst eine Sitzung mit dem Testtreiber starten und dann Skripts ausführen müssen, um GuardDuty Ergebnisse mit bestimmten Ressourcenkombinationen zu generieren.

Teil A — Starten Sie die Sitzung mit dem Testfahrer

1. Nachdem Ihre Ressourcen bereitgestellt wurden, speichern Sie den Regionalcode in einer Variablen in Ihrer aktuellen Terminalsitzung. Verwenden Sie den folgenden Befehl und *us-east-1* ersetzen Sie ihn durch den Regionalcode, für den Sie die Ressourcen bereitgestellt haben:

   ```
   $ REGION=us-east-1
   ```

2. Das Tester-Skript ist nur über AWS Systems Manager (SSM) verfügbar. Um eine interaktive Shell auf der Tester-Host-Instanz zu starten, fragen Sie den Host InstanceIdab.

3. Verwenden Sie den folgenden Befehl, um Ihre Sitzung für das Tester-Skript zu beginnen:

```
aws ssm start-session
  --region $REGION
  --document-name AWS-StartInteractiveCommand
  --parameters command="cd /home/ssm-user/py_tester && bash -l"
  --target $(aws ec2 describe-instances
    --region $REGION
    --filters "Name=tag:Name,Values=Driver-GuardDutyTester"
    --query "Reservations[].Instances[?State.Name=='running'].InstanceId"
    --output text)
```

Teil B — Ergebnisse generieren

Das Tester-Skript ist ein Python-based Programm, das dynamisch ein Bash-Skript erstellt, um Ergebnisse auf der Grundlage Ihrer Eingaben zu generieren. Sie haben die Flexibilität, Ergebnisse auf der Grundlage eines oder mehrerer AWS Ressourcentypen, GuardDuty Schutzpläne, Bedrohungszwecke (Taktiken)Grundlegende Datenquellen, oder the section called “GuardDuty Ergebnisse, die das Tester-Skript generieren kann” zu generieren.

Verwenden Sie die folgenden Befehlsbeispiele als Referenz und führen Sie einen oder mehrere Befehle aus, um Ergebnisse zu generieren, die Sie untersuchen möchten:

```
python3 guardduty_tester.py
python3 guardduty_tester.py --all
python3 guardduty_tester.py --s3
python3 guardduty_tester.py --tactics discovery
python3 guardduty_tester.py --ec2 --eks --tactics backdoor policy execution
python3 guardduty_tester.py --eks --runtime only
python3 guardduty_tester.py --ec2 --runtime only --tactics impact
python3 guardduty_tester.py --log-source dns vpc-flowlogs
python3 guardduty_tester.py --finding 'CryptoCurrency:EC2/BitcoinTool.B!DNS'
```

Weitere Informationen zu gültigen Parametern erhalten Sie, wenn Sie den folgenden Hilfebefehl ausführen:

```
python3 guardduty_tester.py --help
```

Teil C — Überprüfung der generierten Ergebnisse

Wählen Sie eine bevorzugte Methode, um die generierten Ergebnisse in Ihrem Konto anzuzeigen.

GuardDuty console

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Findings aus.
3. Wählen Sie in der Tabelle mit den Ergebnissen ein Ergebnis aus, für das Sie die Details anzeigen möchten. Dadurch wird der Bereich mit den Ergebnisdetails geöffnet. Weitere Informationen finden Sie unter GuardDuty Amazon-Ergebnisse verstehen und generieren.
4. Wenn Sie diese Ergebnisse filtern möchten, verwenden Sie den Ressourcen-Tag key and value. Um beispielsweise die für die Amazon EC2 EC2-Instances generierten Ergebnisse zu filtern, verwenden Sie`CreatedBy: GuardDuty Test Script` tag key:value pair für Instance-Tag-Schlüssel und Instance-Tag-Schlüssel.

API

- Führen Sie ListFindingsden Befehl aus, um die Ergebnisse für eine bestimmte Melder-ID anzuzeigen. Sie können bestimmte Parameter angeben, um die Ergebnisse zu filtern.

  Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

AWS CLI

- Führen Sie den folgenden AWS CLI Befehl aus, um die generierten Ergebnisse anzuzeigen *us-east-1* und *12abc34d567e8fa901bc2d34EXAMPLE* sie durch geeignete Werte zu ersetzen:

```
aws guardduty list-findings --region us-east-1 --detector-
id 12abc34d567e8fa901bc2d34EXAMPLE
```

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

Weitere Informationen zu den Parametern, mit denen Sie Ergebnisse filtern können, finden Sie in der AWS CLI Befehlsreferenz unter list-findings.

Schritt 4 — Testressourcen AWS bereinigen

Die Einstellungen auf Kontoebene und andere Aktualisierungen des Konfigurationsstatus, die während der Schritt 3 — Führen Sie Tester-Skripte aus Rückkehr zum ursprünglichen Zustand vorgenommen wurden, wenn das Tester-Skript abgeschlossen ist.

Nachdem Sie das Tester-Skript ausgeführt haben, können Sie wählen, ob Sie die AWS Testressourcen bereinigen möchten. Sie können sich dafür entscheiden, eine der folgenden Methoden zu verwenden:

- Führen Sie den folgenden Befehl aus:

```
cdk destroy
```

- Löschen Sie den CloudFormation Stapel mit dem Namen GuardDutyTesterStack. Informationen zu den einzelnen Schritten finden Sie unter Löschen eines Stacks auf der CloudFormation Konsole.

Behebung häufiger Probleme

GuardDuty hat häufig auftretende Probleme identifiziert und empfiehlt Schritte zur Fehlerbehebung:

- `Cloud assembly schema version mismatch`— Aktualisieren Sie AWS CDK CLI auf eine Version, die mit der erforderlichen Cloud-Assembly-Version kompatibel ist, oder auf die neueste verfügbare Version. Weitere Informationen finden Sie unter AWS CDK CLI-Kompatibilität.
- `Docker permission denied`— Fügen Sie den Benutzer des dedizierten Kontos zu den Docker - oder Docker-Benutzern hinzu, damit das dedizierte Konto die Befehle ausführen kann. Weitere Informationen zu den einzelnen Schritten finden Sie unter Daemon-Socket-Option.
- `Your requested instance type is not supported in your requested Availability Zone`— Einige Availability Zones unterstützen bestimmte Instanztypen nicht.

Gehen Sie wie folgt vor, um herauszufinden, welche Availability Zones Ihren bevorzugten Instance-Typ unterstützen, und versuchen Sie erneut, AWS Ressourcen bereitzustellen:

1. Wählen Sie eine bevorzugte Methode, um zu ermitteln, welche Availability Zones Ihren Instance-Typ unterstützen:

   Console

   Um Availability Zones zu identifizieren, die den bevorzugten Instance-Typ unterstützen

   1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon EC2 EC2-Konsole unter https://console.aws.amazon.com/ec2/.
   2. Wählen Sie mithilfe der AWS Regionsauswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie die Instance starten möchten.
   3. Wählen Sie im Navigationsbereich unter Instances die Option Instance-Typen aus.
   4. Wählen Sie aus der Tabelle mit den Instanztypen einen bevorzugten Instance-Typ aus.
   5. Sehen Sie sich unter Netzwerk die Regionen an, die unter Availability Zones aufgeführt sind.

      Auf der Grundlage dieser Informationen müssen Sie möglicherweise eine neue Region auswählen, in der Sie die Ressourcen bereitstellen können.

   AWS CLI

   Führen Sie den folgenden Befehl aus, um eine Liste der Availability Zones anzuzeigen. Stellen Sie sicher, dass Sie Ihren bevorzugten Instance-Typ und die Region (*us-east-1*) angeben.

   ```
   aws ec2 describe-instance-type-offerings --location-type availability-zone  --
   filters Name=instance-type,Values=Preferred instance type --region us-east-1 --
   output table
   ```

   Weitere Informationen zu diesem Befehl finden Sie unter describe-instance-type-offers in der Befehlsreferenz.AWS CLI

   Wenn Sie diesen Befehl ausführen und eine Fehlermeldung erhalten, stellen Sie sicher, dass Sie die neueste Version von verwenden. AWS CLI Weitere Informationen finden Sie unter Fehlerbehebung im AWS Command Line Interface -Benutzerhandbuch.

2. Versuchen Sie erneut, die AWS Ressourcen bereitzustellen, und geben Sie eine Availability Zone an, die Ihren bevorzugten Instance-Typ unterstützt.

   Um erneut zu versuchen, Ressourcen bereitzustellen AWS

   1. Richten Sie die Standardregion in der `bin/cdk-gd-tester.ts` Datei ein.
   2. Um die Availability Zone anzugeben, öffnen Sie die `amazon-guardduty-tester/lib/common/network/vpc.ts` Datei.
   3. Ersetzen Sie diese Datei durch die Stelle`maxAzs: 2,` , `availabilityZones: ['us-east-1a', 'us-east-1c'],` an der Sie die Availability Zones für Ihren Instance-Typ angeben müssen.
   4. Fahren Sie mit den verbleibenden Schritten unter fortSchritte zur Bereitstellung von Ressourcen AWS.

Generierte Ergebnisse in der GuardDuty Konsole anzeigen

Wenn eine Aktivität GuardDuty erkannt wird, die dem Muster eines Sicherheitsproblems entspricht, GuardDuty wird ein Ergebnis generiert. Dieses Ergebnis ist mit einem Ressourcentyp verknüpft, der während dieser Aktivität möglicherweise kompromittiert wurde. Sie können die Details zu jedem GuardDuty generierten Ergebnis anzeigen.

Wenn Sie ein GuardDuty Administratorkonto verwenden, können Sie die generierten Ergebnisse im Namen der Mitgliedskonten einsehen. Ein Mitgliedskonto kann jedoch die generierten Ergebnisse in seinem eigenen Konto einsehen. Ein Mitgliedskonto kann die Ergebnisse, die für andere Mitgliedskonten generiert wurden, nicht einsehen.

Schritte zum Anzeigen der Ergebnisse in der GuardDuty Konsole

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im linken Navigationsbereich Ergebnisse aus.

   GuardDuty zeigt die Ergebnisse in tabellarischer Form an. Standardmäßig wird diese Tabelle in absteigender Reihenfolge auf der Grundlage des Spaltenwerts „Zuletzt gesehen“ sortiert, wobei die neuesten Ergebnisse ganz oben angezeigt werden.

Ergebnisse mit einem Schwertsymbol

()

stehen für ein Ergebnis aus einer Angriffssequenz.

3. Um Details zu einem Befund anzuzeigen, wählen Sie dessen Titel aus. Dadurch wird der Seitenbereich mit den Ergebnisdetails geöffnet. Für die Suche nach einer Angriffssequenz enthält dieser Seitenbereich eine Zusammenfassung der Angriffssequenz. Um diese Ansicht zu erweitern, wählen Sie Details anzeigen.

   Informationen zu den in diesem Seitenbereich aufgeführten Feldern finden Sie unterErkenntnisdetails.

4. (Optional), um Finding JSON herunterzuladen

   a. Wählen Sie das Ergebnis aus und wählen Sie dann das Menü Aktionen.

   b. Wählen Sie im Menü „Aktionen“ die Option „JSON anzeigen und exportieren“.

   c. Wählen Sie im JSON-Fenster „Ergebnisse“ die Option „Herunterladen“ aus.

> **Note**
>
> In einigen Fällen GuardDuty wird ihm bewusst, dass es sich bei bestimmten Ergebnissen um falsch positive Ergebnisse handelt, nachdem sie generiert wurden. GuardDuty stellt ein Konfidenzfeld im JSON-Format des Ergebnisses bereit und setzt seinen Wert auf Null. Auf diese Weise GuardDuty wissen Sie, dass Sie solche Ergebnisse getrost ignorieren können.
> Ergebnisse ohne das Feld „Konfidenz“ gelten nicht als falsch positive Ergebnisse.

Auf der Seite „Ergebnisse“ navigieren

Dieser Abschnitt enthält wichtige Informationen zu verschiedenen Elementen auf der Seite „Ergebnisse“. Dies hilft Ihnen bei der Analyse der generierten Ergebnisse für die Bedrohungsanalyse und -abwehr.

In der folgenden Liste werden die Elemente der Ergebnisseite erläutert, anhand derer Sie die generierten Ergebnisse besser verstehen können:

- Art der Bedrohung:

Der Bedrohungstyp umfasst individuelle GuardDuty Ergebnisse und Ergebnisse der Angriffssequenz. Standardmäßig werden auf der Seite Alle Ergebnisse angezeigt.

Um die Tabellenansicht der Ergebnisse zu filtern, wählen Sie im Menü Bedrohungstyp eine der Optionen — Nur Ergebnisse der Angriffssequenz oder Nur einzelne Ergebnisse.

- Spalten „Ressource“ und „Anzahl“:

  In der Spalte Ressource in der Ergebnistabelle wird der Name der potenziell gefährdeten AWS Ressource angezeigt. Bei der Suche nach einer Angriffssequenz wird in dieser Spalte die Anzahl der potenziell gefährdeten Ressourcen AWS angezeigt. Um die Ressourcennamen anzuzeigen, wählen Sie die Zahl in der Spalte Ressource aus.

  Die Spalte Anzahl gibt an, wie oft ein bestimmter Befund GuardDuty beobachtet wurde. Wenn GuardDuty festgestellt wird, dass eine Aktivität mit einem zuvor identifizierten Sicherheitsproblem übereinstimmt, wird die Anzahl für dieses spezielle Ergebnis erhöht. Bei einer Erkennung einer Angriffssequenz gibt dieser Spaltenwert die Gesamtzahl der Signale und Ergebnisse an, die zur Generierung des Ergebnisses beigetragen haben.

- Ergebnisse nach Tabellenspalten sortieren:

  Wenn sich neben einer Spaltenüberschrift ein Pfeil befindet, können Sie die Ergebnistabelle anhand der Spalte sortieren. Wählen Sie die Spaltenüberschrift aus, um die Ergebnisse entweder in aufsteigender oder absteigender Reihenfolge des Werts in dieser Spalte zu sortieren.

- Ergebnisse filtern:

  Basierend auf bestimmten Eigenschaftsattributen wie `Account ID` und `Resource type` können Sie die Ergebnistabelle weiter filtern. Informationen zu den Filtertypen, die Sie verwenden können, finden Sie unter GuardDuty Ergebnisse filtern.

- Status und gespeicherte Regeln:

  Das Statusmenü enthält zwei Werte — Aktuell und Archiviert. Die Standardansicht ist Aktuelle Ergebnisse in der Tabelle.

  Wenn Sie kein Ergebnis mehr generieren GuardDuty möchten, das einem bestimmten Kriterium entspricht, können Sie dieses Ergebnis unterdrücken. GuardDuty archiviert diesen Befund. Wenn dieser Befund erneut GuardDuty erkannt wird, werden Sie nicht über diese Beobachtung informiert. Um speziell archivierte Ergebnisse anzuzeigen, wählen Sie im Menü Status die Option Archiviert aus.

Gespeicherte Regeln sind eine Funktion, mit der Sie Ergebnisse, die bestimmten Kriterien entsprechen, automatisch filtern und Maßnahmen ergreifen können. Zu den Aktionen können das Archivieren von Ergebnissen oder das Ausblenden dieser Ergebnisse aus zukünftigen Benachrichtigungen gehören.

Weitere Informationen finden Sie unter Unterdrückungsregeln.

Schweregrad der Ergebnisse GuardDuty

Jedem GuardDuty Befund ist ein Schweregrad und ein Wert zugewiesen, der das potenzielle Risiko widerspiegelt, das das Ergebnis für Ihre Umgebung darstellen könnte. Dies wurde von unseren Sicherheitstechnikern festgestellt. Der Schweregrad kann zwischen 1,0 und 10,0 liegen, wobei höhere Werte auf ein größeres Sicherheitsrisiko hinweisen. Unterteilen Sie diesen Bereich in die Schweregrade „Kritisch“, „Hoch“, „Mittel“ und „Niedrig“, GuardDuty um Ihnen zu helfen, die Reaktion auf ein potenzielles Sicherheitsproblem zu ermitteln, das durch ein Ergebnis hervorgehoben wird.

Ein Befund eines bestimmten Typs kann je nach Kontext, in dem das Ergebnis vorliegt, einen anderen Schweregrad haben. Eine konsolidierte Liste der Standardschweregrade für alle GuardDuty Befundarten finden Sie unterGuardDuty Typen von aktiven Ergebnissen.

In den folgenden Abschnitten werden die für die GuardDuty Ergebnisse definierten Schweregrade erläutert.

Themen

- Kritischer Schweregrad
- Hoher Schweregrad
- Mittlerer Schweregrad
- Niedriger Schweregrad

Kritischer Schweregrad

Wertebereich: 9,0 — 10,0

Beschreibung: Ein kritischer Schweregrad gibt an, dass eine Angriffssequenz möglicherweise im Gange ist oder kürzlich stattgefunden hat. Eine oder mehrere AWS Ressourcen, wie z. B. die Anmeldeinformationen eines IAM-Benutzers und der Amazon S3-Bucket, sind möglicherweise gefährdet oder wurden bereits kompromittiert.

Empfehlung: GuardDuty empfiehlt, dass Sie der Prüfung und Behebung aller Befunde mit kritischem Schweregrad Priorität einräumen, da diese Probleme Teil eines Ransomware-Angriffs sein können und jederzeit eskalieren können. Sehen Sie sich Details zu den beteiligten Ressourcen an und beginnen Sie mit der Behebung der Sicherheitsprobleme. Weitere Informationen finden Sie unter Behebung von Erkenntnissen.

Hoher Schweregrad

Wertebereich: 7,0 - 8,9

Beschreibung: Ein hoher Schweregrad gibt an, dass die fragliche Ressource (eine Amazon EC2-Instance oder eine Reihe von IAM-Benutzeranmeldedaten) kompromittiert ist und aktiv für nicht autorisierte Zwecke verwendet wird.

Empfehlung: GuardDuty empfiehlt, jedes Sicherheitsproblem mit hohem Schweregrad als Priorität zu behandeln und sofortige Abhilfemaßnahmen zu ergreifen, um eine weitere unbefugte Nutzung Ihrer Ressourcen zu verhindern. Bereinigen Sie beispielsweise Ihre Amazon EC2-Instance oder beenden Sie sie oder rotieren Sie die IAM-Anmeldeinformationen. Folgen Sie den Schritten unter, um den Behebung von Erkenntnissen Befund zu korrigieren.

Mittlerer Schweregrad

Wertebereich: 4,0 — 6,9

Beschreibung: Ein mittlerer Schweregrad weist auf verdächtige Aktivitäten hin, die vom normalerweise beobachteten Verhalten abweichen und je nach Anwendungsfall auf eine Gefährdung der Ressourcen hinweisen können.

Empfehlung: GuardDuty empfiehlt, die potenziell betroffene Ressource so bald wie möglich zu untersuchen. Die Schritte zur Behebung variieren je nach Ressource und Suche nach einer Familie. Bei einem etablierten Ansatz müssen Sie sicherstellen, dass die Aktivität autorisiert ist und Ihrem Anwendungsfall entspricht. Wenn Sie die Ursache nicht identifizieren oder nicht bestätigen können, dass die Aktivität autorisiert wurde, sollten Sie davon ausgehen, dass die Ressource gefährdet ist. Folgen Sie den Schritten unterBehebung von Erkenntnissen, um den Befund zu korrigieren.

Bei der Überprüfung eines mittelgradigen Ergebnisses sollten Sie Folgendes beachten:

- Prüfen Sie, ob ein autorisierter Benutzer neue Software installiert hat, die das Verhalten einer Ressource ändert (z. B. mehr Datenverkehr als normal zugelassen oder die Kommunikation über einen neuen Port aktiviert hat).

- Prüfen Sie, ob ein autorisierter Benutzer die Einstellungen der Kontrollebene geändert hat, z. B. eine Sicherheitsgruppeneinstellung geändert hat.
- Führen Sie eine Virenprüfung der betroffenen Ressource durch, um nicht autorisierte Software zu erkennen.
- Überprüfen Sie die Berechtigungen, die mit der betroffenen IAM-Rolle, dem Benutzer, der Gruppe oder den Anmeldeinformationen verbunden sind. Möglicherweise müssen diese geändert oder rotiert werden.

Niedriger Schweregrad

Wertebereich: 1,0 - 3,9

Beschreibung: Ein niedriger Schweregrad weist auf versuchte verdächtige Aktivitäten hin, die Ihre Umgebung nicht beeinträchtigt haben, z. B. ein Port-Scan oder ein fehlgeschlagener Eindringversuch.

Empfehlung: Es gibt keine unmittelbare Handlungsempfehlung, aber es lohnt sich, diese Informationen zur Kenntnis zu nehmen, da sie darauf hindeuten können, dass jemand nach Schwachstellen in Ihrer Umgebung sucht.

Erkenntnisdetails

In der GuardDuty Amazon-Konsole können Sie die Details zu den Ergebnissen im Abschnitt Zusammenfassung der Ergebnisse einsehen. Die Erkenntnisdetails variieren je nach Erkenntnistyp.

Hauptsächlich bestimmen zwei Details, welche Arten von Informationen für jede Erkenntnis verfügbar sind. Der erste ist der Ressourcentyp, der`Instance`,`AccessKey`,`S3Bucket`,`S3Object`,`Kubernetes cluster`,`ECS cluster`, `Container` `RDSDBInstance``RDSLimitlessDB`, oder sein kann`Lambda`. Das zweite Detail, das die Suche nach Informationen bestimmt, ist die Ressourcenrolle. Die Rolle der Ressource kann sein`Target`, was bedeutet, dass die Ressource das Ziel verdächtiger Aktivitäten war. Bei Feststellungen vom Typ Instance kann die Rolle der Ressource auch `Actor` sein, was bedeutet, dass Ihre Ressource der Akteur war, der die verdächtige Aktivität durchgeführt hat. In diesem Thema werden einige der allgemein verfügbaren Erkenntnisdetails beschrieben. Für the section called “Bei der Laufzeitüberwachung werden Typen gefunden” und Suchtyp „Malware-Schutz für S3“ ist die Ressourcenrolle nicht gefüllt.

Themen

- Überblick über Erkenntnisse
- Ressource
- Einzelheiten zur Suche nach der Angriffssequenz
- Benutzerdetails für die RDS-Datenbank (DB)
- Details zu den Erkenntnissen der Laufzeitüberwachung
- Scan-Details der EBS-Volumes
- Einzelheiten zur Suche nach Malware Protection for EC2
- Einzelheiten zu Erkenntnissen von Malware Protection für S3
- Action
- Akteur oder Ziel
- Einzelheiten zur Geolokalisierung
- Zusätzliche Informationen
- Beweise
- Anormales Verhalten

Überblick über Erkenntnisse

Der Abschnitt Überblick enthält die grundlegendsten Merkmale, anhand derer die Erkenntnis identifiziert werden kann, einschließlich der folgenden Informationen:

- Konto-ID — Die ID des AWS Kontos, in dem die Aktivität stattfand, die GuardDuty zur Generierung dieses Ergebnisses geführt hat.
- Anzahl — Gibt an, wie oft GuardDuty eine Aktivität, die diesem Muster entspricht, mit dieser Ergebnis-ID aggregiert wurde.
- Erstellt am – Uhrzeit und Datum des Zeitpunkts, an dem diese Erkenntnis erstmals erstellt wurde. Wenn dieser Wert von Aktualisiert am abweicht, bedeutet dies, dass die Aktivität mehrfach stattgefunden hat und ein fortlaufendes Problem darstellt.

> **Note**
>
> Zeitstempel für Ergebnisse in der GuardDuty Konsole werden in Ihrer lokalen Zeitzone angezeigt, während JSON-Exporte und CLI-Ausgaben Zeitstempel in UTC anzeigen.

- Erkenntnis-ID – Eine eindeutige Erkenntnis-ID für diesen Erkenntnistyp und Parametersatz. Neue Vorkommen von Aktivitäten, die diesem Muster entsprechen, werden für dieselbe ID aggregiert.
- Erkenntnistyp – Eine formatierte Zeichenfolge, die den Typ der Aktivität darstellt, durch den die Erkenntnis ausgelöst wurde. Weitere Informationen finden Sie unter GuardDuty Format finden.
- Region — Die AWS Region, in der das Ergebnis generiert wurde. Weitere Informationen zu unterstützten Regionen finden Sie unter Regionen und Endpunkte
- Ressourcen-ID — Die ID der AWS Ressource, für die die Aktivität stattgefunden hat, die GuardDuty zur Generierung dieses Ergebnisses geführt hat.
- Scan-ID — Gilt für Ergebnisse, wenn GuardDuty Malware Protection for EC2 aktiviert ist. Dabei handelt es sich um eine Kennung des Malware-Scans, der auf den EBS-Volumes ausgeführt wird, die an die potenziell gefährdete EC2-Instance oder den Container-Workload angehängt sind. Weitere Informationen finden Sie unter Einzelheiten zur Suche nach Malware Protection for EC2.
- Schweregrad — Einem Ergebnis wird entweder der Schweregrad Kritisch, Hoch, Mittel oder Niedrig zugewiesen. Weitere Informationen finden Sie unter Schweregrad der Ergebnisse.
- Aktualisiert am — Das letzte Mal, als dieses Ergebnis mit einer neuen Aktivität aktualisiert wurde, die dem Muster entspricht, das GuardDuty zur Generierung dieses Ergebnisses geführt hat.

Ressource

Die betroffene Ressource enthält Einzelheiten zu der AWS Ressource, auf die die auslösende Aktivität abzielte. Die verfügbaren Informationen variieren je nach Ressourcentyp und Aktionstyp.

Ressourcenrolle — Die Rolle der AWS Ressource, die den Befund ausgelöst hat. Dieser Wert kann TARGET oder ACTOR lauten und repräsentiert, ob Ihre Ressource das Ziel verdächtiger Aktivitäten bzw. der Akteur war, der die verdächtigen Aktivitäten ausgeführt hat.

Ressourcen-Typ – der Typ der betroffenen Ressource. Wenn mehrere Ressourcen betroffen waren, kann eine Erkenntnis mehrere Ressourcentypen umfassen. Die Ressourcentypen sind Instance, S3Bucket AccessKey, S3Object, ECSCluster, Container, RDSDBInstance KubernetesCluster, RdsLimitlessDB und Lambda. Je nach Ressourcentyp stehen unterschiedliche Erkenntnisdetails zur Verfügung. Wählen Sie eine Registerkarte mit Ressourcenoptionen aus, um mehr über die für diese Ressource verfügbaren Details zu erfahren.

Instance

Instance-Details:

> **Note**
>
> Einige Instance-Details fehlen möglicherweise, wenn die Instance bereits gestoppt wurde oder wenn der zugrunde liegende API-Aufruf bei einem regionsübergreifenden API-Aufruf von einer EC2-Instance in einer anderen Region stammte.

- Instanz-ID — Die ID der EC2-Instance, die an der Aktivität beteiligt war, die zur Generierung des Ergebnisses geführt hat. GuardDuty
- Instance-Typ – Der Typ der EC2-Instance, der an der Erkenntnis beteiligt ist.
- Startzeit – Das Datum und die Uhrzeit, zu der die Instance gestartet wurde.
- Outpost ARN — Der Amazon-Ressourcenname (ARN) von AWS Outposts. Gilt nur für AWS Outposts Instances. Weitere Informationen finden Sie unter Was ist AWS Outposts? im Benutzerhandbuch für Outposts-Racks.
- Name der Sicherheitsgruppe – Der Name der Sicherheitsgruppe, die der beteiligten Instance angefügt ist.
- Sicherheitsgruppen-ID – Die ID der Sicherheitsgruppe, die der beteiligten Instance angefügt ist.
- Instance-Status – Der aktuelle Status der Ziel-Instance.
- Availability Zone – Die Availability Zone der AWS -Region, in der sich die betroffene Instance befindet.
- Image-ID – Die ID des Amazon Machine Image, das zum Erstellen der an der Aktivität beteiligten Instance verwendet wurde.
- Image-Beschreibung – Eine Beschreibung der ID des Amazon Machine Image, das zum Erstellen der Instance verwendet wurde, die an der Aktivität beteiligt war.
- Tags – Eine Liste der Tags, die dieser Ressource angefügt sind, die im Format `key:value` aufgeführt werden.

AccessKey

Details zu Zugriffsschlüsseln:

- Zugriffsschlüssel-ID — Die Zugriffsschlüssel-ID des Benutzers, der an der Aktivität beteiligt war, die GuardDuty zur Generierung des Ergebnisses geführt hat.
- Prinzipal-ID — Die Prinzipal-ID des Benutzers, der an der Aktivität beteiligt war, die GuardDuty zur Generierung des Ergebnisses geführt hat.

- Benutzertyp — Der Benutzertyp, der an der Aktivität beteiligt war, die GuardDuty zur Generierung des Ergebnisses geführt hat. Weitere Informationen finden Sie unter CloudTrail - Element userIdentity.
- Benutzername — Der Name des Benutzers, der an der Aktivität beteiligt war, die GuardDuty zur Generierung des Ergebnisses geführt hat.

S3Bucket

Details zum Amazon-S3-Bucket:

- Name – Der Name des Buckets, der an der Erkenntnis beteiligt war.
- ARN – Der ARN des Buckets, der an der Erkenntnis beteiligt war.
- Eigentümer – Die kanonische Benutzer-ID des Benutzers, dem der Bucket gehört, der an der Erkenntnis beteiligt war. Weitere Informationen zu kanonischen Benutzer-IDs finden Sie unter AWS -Konto-Kennungen.
- Typ – Der Typ der Bucket-Erkenntnis. Mögliche Werte sind Ziel oder Quelle.
- Standardmäßige serverseitige Verschlüsselung – Verschlüsselungsdetails für den Bucket.
- Bucket-Tags – Eine Liste der Tags, die dieser Ressource zugeordnet sind und im Format `key:value` aufgeführt werden.
- Effektive Berechtigungen – Eine Auswertung aller effektiven Berechtigungen und Richtlinien für den Bucket, die angibt, ob der betreffende Bucket öffentlich verfügbar ist. Werte können Öffentlich oder Nicht öffentlich sein.

S3Object

- S3-Objektdetails — Enthält die folgenden Informationen über das gescannte S3-Objekt:
  - ARN — Amazon-Ressourcenname (ARN) des gescannten S3-Objekts.
  - Schlüssel — Der Name, der der Datei zugewiesen wurde, als sie im S3-Bucket erstellt wurde.
  - Versions-ID — Wenn Sie die Bucket-Versionierung aktiviert haben, gibt dieses Feld die Versions-ID an, die der neuesten Version des gescannten S3-Objekts zugeordnet ist. Weitere Informationen finden Sie unter Verwenden der Versionierung in S3-Buckets im Amazon S3 S3-Benutzerhandbuch.
  - ETag — Stellt die spezifische Version des gescannten S3-Objekts dar.
  - Hash — Der Hash der Bedrohung, die in diesem Ergebnis erkannt wurde.

- S3-Bucket-Details — Enthält die folgenden Informationen über den Amazon S3 S3-Bucket, der dem gescannten S3-Objekt zugeordnet ist:
  - Name — Gibt den Namen des S3-Buckets an, der das Objekt enthält.
  - ARN — Amazon-Ressourcenname (ARN) des S3-Buckets.
- Besitzer — Kanonische ID des Besitzers des S3-Buckets.

EKSCluster

Details zum Kubernetes-Cluster:

- Name – Name des Kubernetes-Clusters.
- ARN – Der ARN, der den Cluster identifiziert.
- Erstellt am – Uhrzeit und Datum des Zeitpunkts, an dem dieser Cluster erstmals erstellt wurde.

  > **Note**
  >
  > Zeitstempel für Ergebnisse in der GuardDuty Konsole werden in Ihrer lokalen Zeitzone angezeigt, während JSON-Exporte und CLI-Ausgaben Zeitstempel in UTC anzeigen.

- VPC-ID – Die ID der VPC, die Ihrem Cluster zugeordnet ist.
- Status – Der aktuelle Status des Clusters.
- Tags – Die Metadaten, die Sie auf den Cluster anwenden, um die Kategorisierung und Organisation zu erleichtern. Jedes Tag besteht aus einem Schlüssel und einem optionalen Wert, aufgelistet im Format `key:value`. Sie können sowohl den Schlüssel als auch den Wert definieren.

  Cluster-Tags werden nicht auf andere Ressourcen verteilt, die dem Cluster zugeordnet sind.

Details zum Kubernetes-Workload:

- Typ – Der Typ des Kubernetes-Workloads, wie Pod, Bereitstellung und Job.
- Name – Der Name des Kubernetes-Workloads.
- Uid – Die eindeutige ID des Kubernetes-Workloads.
- Erstellt am – Uhrzeit und Datum des Zeitpunkts, an dem dieser Workload erstmals erstellt wurde.
- Labels – Die Schlüssel-Wert-Paare, die dem Kubernetes-Workload angefügt wurden.

- Container – Die Details des Containers, der als Teil des Kubernetes-Workloads ausgeführt wird.
- Namespace – Der Workload gehört zu diesem Kubernetes-Namespace.
- Volumes – Die vom Kubernetes-Workload verwendeten Volumes.
  - Hostpfad – Stellt eine bereits vorhandene Datei oder ein Verzeichnis auf dem Host-Computer dar, dem das Volume zugeordnet ist.
  - Name – Der Name des Volumes.
- Pod-Sicherheitskontext – Definiert die Einstellungen für Rechte und Zugriffskontrolle für alle Container in einem Pod.
- Host-Netzwerk – Auf `true` setzen, wenn die Pods im Kubernetes-Workload enthalten sind.

Kubernetes-Benutzerdetails:

- Gruppen – Kubernetes-RBAC (Role-Access Based Control)-Gruppen des Benutzers, der an der Aktivität beteiligt war, die die Erkenntnis generiert hat.
- ID – Eindeutige ID des Kubernetes-Benutzers.
- Benutzername – Name des Kubernetes-Benutzers, der an der Aktivität beteiligt war, die das Ergebnis generiert hat.
- Sitzungsname – Entität, die die IAM-Rolle mit Kubernetes-RBAC-Berechtigungen übernommen hat.

ECSCluster

ECS-Cluster-Details:

- ARN – Der ARN, der den Cluster identifiziert.
- Name – Der Name des Clusters.
- Status – Der aktuelle Status des Clusters.
- Anzahl der aktiven Services – Die Anzahl der Services, die in einem `ACTIVE`-Status auf dem Cluster ausgeführt werden. Sie können diese Dienste mit anzeigen ListServices
- Anzahl registrierter Container-Instances – Die Anzahl der Container-Instances, die im Cluster registriert sind. Dazu gehören Container-Instances sowohl im Status `ACTIVE` als auch im Status `DRAINING`.
- Anzahl der laufenden Aufgaben – Die Anzahl der Aufgaben im Cluster, die sich im `RUNNING`-Status befinden.

- Tags – Die Metadaten, die Sie auf den Cluster anwenden, um die Kategorisierung und Organisation zu erleichtern. Jedes Tag besteht aus einem Schlüssel und einem optionalen Wert, aufgelistet im Format `key:value`. Sie können sowohl den Schlüssel als auch den Wert definieren.
- Container – Die Details zu dem Container, der der Aufgabe zugeordnet ist:
  - Containername – Der Name des Containers.
  - Container-Image – Das Image des Containers.
- Aufgabendetails – Die Details einer Aufgabe in einem Cluster.
  - ARN – Der Amazon-Ressourcenname (ARN) der Aufgabe.
  - Definition-ARN – Der Amazon-Ressourcenname (ARN) der Aufgabendefinition, die die Aufgabe erstellt.
  - Version – Der Versionszähler für die Aufgabe.
  - Aufgabe erstellt am – Der Unix-Zeitstempel für den Erstellungszeitpunkt der Aufgabe.
  - Aufgabe gestartet am – Der Unix-Zeitstempel für den Startzeitpunkt der Aufgabe.
  - Aufgabe gestartet von – Das Tag, das beim Starten einer Aufgabe angegeben wurde.

Container

Details zum Container:

- Container-Laufzeit – Die Container-Laufzeit (wie z. B. `docker` oder `containerd`), die zum Ausführen des Containers verwendet wurde.
- ID – Die Container-Instance-ID oder die vollständigen ARN-Einträge für die Container-Instance.
- Name – Der Name des Containers.
- Image – Das Image der Container-Instance.
- Volume-Mounts – Liste der Volume-Mounts von Containern. Ein Container kann ein Volume unter seinem Dateisystem mounten.
- Sicherheitskontext – Der Sicherheitskontext des Containers definiert Einstellungen für Rechte und Zugriffskontrolle für einen Container.
- Prozessdetails – Beschreibt die Details des Prozesses, der mit der Erkenntnis verknüpft ist.

RDSDBInstance

Details zur RDSDBInstance:

> **Note**
>
> Diese Ressource ist in den Erkenntnissen von RDS Protection im Zusammenhang mit der Datenbank-Instance verfügbar.

- Datenbankinstanz-ID — Der Bezeichner, der der Datenbankinstanz zugeordnet ist, die an der GuardDuty Suche beteiligt war.
- Engine – Der Name der Datenbank-Engine der Datenbank-Instance, die an der Erkenntnis beteiligt war. Mögliche Werte sind Aurora MySQL-Compatible oder Aurora PostgreSQL-Compatible.
- Engine-Version — Die Version der Datenbank-Engine, die an der GuardDuty Entdeckung beteiligt war.
- Datenbank-Cluster-ID — Der Bezeichner des Datenbank-Clusters, der die Datenbank-Instance-ID enthält, die an der GuardDuty Suche beteiligt war.
- Datenbankinstanz-ARN — Der ARN, der die an der GuardDuty Suche beteiligte Datenbankinstanz identifiziert.

RDSLimitlessDB

Einzelheiten zu RdsLimitlessDB:

Diese Ressource ist in den Ergebnissen von RDS Protection verfügbar, die sich auf die unterstützte Engine-Version von Limitless Database beziehen.

- DB-Shard-Gruppen-ID — Der Name, der der Limitless-DB-Shard-Gruppe zugeordnet ist.
- Ressourcen-ID der DB-Shardgruppe — Die Ressourcen-ID der DB-Shard-Gruppe innerhalb der Limitless DB.
- ARN der DB-Shard-Gruppe — Der Amazon-Ressourcenname (ARN), der die DB-Shard-Gruppe identifiziert.
- Engine — Die Kennung der Limitless-DB, die an der Entdeckung beteiligt war.
- Engine-Version — Die Version der Limitless DB-Engine.
- DB-Cluster-ID — Der Name des Datenbank-Clusters, der Teil der Limitless DB ist.

Hinweise zu Benutzer- und Authentifizierungsdetails der potenziell betroffenen Datenbank finden Sie unter. Benutzerdetails für die RDS-Datenbank (DB)

Lambda

Details zur Lambda-Funktion

- Funktionsname – Der Name der Lambda-Funktion, die an der Erkenntnis beteiligt ist.
- Funktionsversion – Die Version der Lambda-Funktion, die an der Erkenntnis beteiligt ist.
- Funktionsbeschreibung – Eine Beschreibung der Lambda-Funktion, die an der Erkenntnis beteiligt ist.
- Funktions-ARN – Der Amazon-Ressourcenname (ARN) der Lambda-Funktion, die an der Erkenntnis beteiligt ist.
- Revisions-ID – Die Revisions-ID der Lambda-Funktionsversion.
- Rolle – Die Ausführungsrolle der Lambda-Funktion, die an der Erkenntnis beteiligt ist.
- VPC-Konfiguration – Die Amazon-VPC-Konfiguration, einschließlich der VPC-ID, Sicherheitsgruppe und Subnetz-IDs, die Ihrer Lambda-Funktion zugeordnet sind.
  - VPC-ID – Die ID der Amazon-VPC, die der Lambda-Funktion zugeordnet ist, die an der Erkenntnis beteiligt ist.
  - Subnetz-IDs – Die IDs der Subnetze, die Ihrer Lambda-Funktion zugeordnet sind.
  - Sicherheitsgruppe – Die Sicherheitsgruppe, die der betroffenen Lambda-Funktion angefügt ist. Dazu gehören der Name und die Gruppen-ID der Sicherheitsgruppe.
- Tags – Eine Liste der Tags, die dieser Ressource angefügt sind, die im Format `key:value` aufgeführt werden.

Einzelheiten zur Suche nach der Angriffssequenz

GuardDuty bietet Details zu jedem Befund, den es in Ihrem Konto generiert. Diese Informationen helfen Ihnen dabei, die Gründe für den Befund zu verstehen. Dieser Abschnitt konzentriert sich auf Details im Zusammenhang mitArten der Suche nach Angriffssequenzen. Dazu gehören Erkenntnisse wie potenziell betroffene Ressourcen, der Zeitplan der Ereignisse, Indikatoren, Signale und Endpunkte, die an den Ergebnissen beteiligt waren.

Einzelheiten zu Signalen, bei denen es sich um GuardDuty Ergebnisse handelt, finden Sie in den entsprechenden Abschnitten auf dieser Seite.

Wenn Sie in der GuardDuty Konsole ein Ergebnis der Angriffssequenz auswählen, ist der Seitenbereich mit den Details in die folgenden Registerkarten unterteilt:

- Überblick — Bietet eine kompakte Ansicht der Details zur Angriffssequenz, einschließlich Signalen, MITRE-Taktiken und potenziell betroffenen Ressourcen.
- Signale — Zeigt eine Zeitleiste der Ereignisse an, die an einer Angriffssequenz beteiligt sind.
- Ressourcen — Stellt Informationen zu den potenziell betroffenen oder potenziell gefährdeten Ressourcen bereit.

Die folgende Liste enthält Beschreibungen im Zusammenhang mit den Details zur Entdeckung der Angriffssequenz.

Signale

Bei einem Signal kann es sich um eine API-Aktivität oder um einen Befund handeln, der zur Erkennung einer Angriffssequenz GuardDuty verwendet wird. GuardDuty betrachtet die schwachen Signale, die sich nicht als eindeutige Bedrohung darstellen, fügt sie zusammen und korreliert mit individuell generierten Ergebnissen. Für mehr Kontext bietet die Registerkarte „Signale“ eine Zeitleiste der Signale, wie sie von GuardDuty beobachtet wurden.

Jedem Signal, also einem GuardDuty Befund, ist ein eigener Schweregrad und ein eigener Wert zugewiesen. In der GuardDuty Konsole können Sie jedes Signal auswählen, um die zugehörigen Details anzuzeigen.

Schauspieler

Enthält Einzelheiten zu den Bedrohungsakteuren in einer Angriffssequenz. Weitere Informationen finden Sie unter Actor in Amazon GuardDuty API Reference.

Endpunkte

Enthält Details zu den Netzwerkendpunkten, die in dieser Angriffssequenz verwendet wurden. Weitere Informationen finden Sie NetworkEndpointunter Amazon GuardDuty API Reference. Informationen darüber, wie der Standort GuardDuty bestimmt wird, finden Sie unterEinzelheiten zur Geolokalisierung.

Indikatoren

Beinhaltet beobachtete Daten, die dem Muster eines Sicherheitsproblems entsprechen. Diese Daten geben an, warum GuardDuty es Hinweise auf eine potenziell verdächtige Aktivität gibt.

Lautet der Indikatorname beispielsweise`HIGH_RISK_API`, deutet dies auf eine Aktion hin, die häufig von Bedrohungsakteuren verwendet wird, oder auf eine sensible Aktion, die potenzielle Auswirkungen auf eine haben kann AWS-Konto, z. B. den Zugriff auf Anmeldeinformationen oder die Änderung einer Ressource.

Die folgende Tabelle enthält eine Liste potenzieller Indikatoren und deren Beschreibungen:

Name des Indikators	Description
`ATTACK_TACTIC`	Die MITRE-Taktik, die der Bedrohungsakteur in einer Angriffssequenz verwendet. Zu den Beispielen gehören Discovery und Impact.
`ATTACK_TECHNIQUE`	Die MITRE-Technik, die vom Bedrohungsakteur in einer Angriffssequenz verwendet wird. Beispiele hierfür sind der Zugriff auf Ressourcen und deren unbeabsichtigte Verwendung sowie das Ausnutzen von Sicherheitslücken.
`CRYPTOMINING_DOMAIN`	Zeigt einen Domainnamen an, der mit Mining-Pools oder Infrastrukturen für Kryptowährungen verknüpft ist. Beispielsweise können DNS-Abfragen oder Verbindungen zu diesen Domains aus Container- oder Kubernetes-Umgebungen auf unbefugte Cryptomining-Aktivitäten hinweisen.
`CRYPTOMINING_IP`	Zeigt eine IP-Adresse an, die mit Kryptowährungs-Mining-Pools oder der Infrastruktur verknüpft ist. Beispielsweise können Verbindungen zu diesen Adressen aus Container- oder Kubernetes-Umgebungen auf unbefugte Cryptomining-Aktivitäten hinweisen.
`CRYPTOMINING_PROCESS`	Weist auf einen Prozess hin, der als Cryptocurrency-Mining-Software identifiziert wurde und in Container- oder Kubernetes-Umgebungen ausgeführt wird. Diese Prozesse können beispielsweise übermäßige CPU-Ressourcen verbrauchen.
`HIGH_RISK_API`	Die AWS API, die den AWS-Service Namen enthält und `eventName` auf eine Aktion hinweist, die häufig von Bedrohungsakteuren verwendet wird, oder es handelt sich um eine sensible Aktion, die potenzielle Auswirkungen haben kann AWS-Konto, z. B. den Zugriff auf Anmeldeinformationen oder die Änderung von Ressourcen.

Name des Indikators	Description
MALICIOUS_DOMAIN	Weist auf einen Domainnamen mit vermuteten Bedrohungsinformationen hin, die auf böswillige Absichten hinweisen. Dazu gehören beispielsweise Command-and-Control-Server (C&C), Websites zur Verbreitung von Schadsoftware oder Phishing-Domänen, die von Container- oder Kubernetes-Umgebungen aus kontaktiert werden.
MALICIOUS_FILE	Weist auf eine Datei hin, bei der aufgrund von Bedrohungsinformationen oder Verhaltensanalysen der Verdacht besteht, dass sie bösartig ist. Dazu gehören beispielsweise bekannte Malware-Binärdateien, bösartige Skripts oder nicht autorisierte ausführbare Dateien.
MALICIOUS_IP	Die IP-Adresse enthält bestätigte Bedrohungsinformationen, die auf böswillige Absichten hinweisen.
MALICIOUS_PACKAGE	Zeigt an, dass eine an der Angriffssequenz beteiligte Ressource ein als bösartig identifiziertes Softwarepaket enthält. Zu den Indikatorwerten gehören bösartige Paketkennungen, die die OSV-Bezeichnung (MAL-*) verwenden, die den erkannten Paketen zugeordnet sind.
MALICIOUS_PROCESS	Weist auf einen Prozess hin, bei dem aufgrund von Bedrohungsinformationen oder Verhaltensanalysen vermutet wird, dass er bösartig ist. Dazu gehören beispielsweise bekannte Malware, Backdoors oder nicht autorisierte Tools, die innerhalb einer Instance- oder Container-Umgebung ausgeführt werden.
MISCONFIGURATION	Weist darauf hin, dass eine an der Angriffssequenz beteiligte Ressource eine Sicherheitsfehlkonfiguration aufweist, die die potenziellen Auswirkungen erhöhen kann. Beispiele hierfür sind administrative Zugriffsrichtlinien, deaktivierte Versionierung oder fehlende Verschlüsselung. Diese Fehlkonfigurationen werden durch identifiziert. AWS Security Hub CSPM Weitere Informationen finden Sie im AWS Security Hub CSPM Benutzerhandbuch unter Unterstützte Eigenschaftstypen.

Name des Indikators	Description
REACHABILITY	Zeigt an, dass eine an der Angriffssequenz beteiligte Ressource über das Internet erreichbar oder öffentlich zugänglich ist. Beispiele hierfür sind über das Internet erreichbare Amazon EC2 EC2-Instances, Amazon EKS-Cluster, Amazon ECS-Cluster oder öffentlich zugängliche Amazon S3 S3-Buckets. Weitere Informationen finden Sie im Benutzerhandbuch unter Unterstützte Merkmalstypen.AWS Security Hub CSPM
SENSITIVE_DATA	Weist darauf hin, dass ein Amazon S3 S3-Bucket, der an der Angriffssequenz beteiligt ist, sensible Daten enthält, wie sie von Amazon Macie identifiziert wurden. AWS Security Hub CSPM
SUSPICIOUS_NETWORK	Das Netzwerk wird mit bekanntermaßen niedrigen Reputationswerten in Verbindung gebracht, z. B. bei riskanten VPN-Anbietern (Virtual Private Network) und Proxydiensten.
SUSPICIOUS_PROCESS	Weist auf einen verdächtigen Prozess hin, der auf der Grundlage von Bedrohungsinformationen oder Verhaltensanalysen als anomal identifiziert wurde. Dazu gehören beispielsweise ungewöhnliche Muster bei der Prozessausführung, unerwartete Beziehungen zwischen übergeordneten und untergeordneten Elementen oder Prozesse mit verdächtigen Merkmalen innerhalb einer Instance- oder Containerumgebung.
SUSPICIOUS_USER_AGENT	Der Benutzeragent ist mit potenziell bekannten verdächtigen oder ausgenutzten Anwendungen wie Amazon S3 S3-Clients und Angriffstools verknüpft.
TOR_IP	Die IP-Adresse ist einem Tor-Ausgangsknoten zugeordnet.
UNUSUAL_API_FOR_ACCOUNT	Zeigt an, dass die AWS API ungewöhnlich aufgerufen wurde, basierend auf der historischen Ausgangsbasis des Kontos. Weitere Informationen finden Sie unter Anormales Verhalten.

Name des Indikators	Description
`UNUSUAL_ASN_FOR_ACCOUNT`	Zeigt an, dass die Autonome Systemnummer (ASN) auf der Grundlage des historischen Basiswerts des Kontos als ungewöhnlich eingestuft wurde. Weitere Informationen finden Sie unter Anormales Verhalten.
`UNUSUAL_ASN_FOR_USER`	Zeigt an, dass die Autonome Systemnummer (ASN) auf der Grundlage des historischen Ausgangswerts des Benutzers als ungewöhnlich eingestuft wurde. Weitere Informationen finden Sie unter Anormales Verhalten.
`VULNERABILITY`	Weist darauf hin, dass eine an der Angriffssequenz beteiligte Ressource bekannte Sicherheitslücken mit kritischem, hohem, mittlerem oder niedrigem Schweregrad aufweist. Die Indikatorwerte umfassen CVE-Identifikatoren und deren Schweregrad. Diese Sicherheitslücken werden von Amazon Inspector erkannt und können die potenziellen Auswirkungen der Angriffssequenz erhöhen. Weitere Informationen zu Schweregraden finden Sie unter Grundlegendes zu Schweregraden im Amazon Inspector Inspector-Benutzerhandbuch.

MITRE-Taktiken

Dieses Feld spezifiziert die MITRE ATT&CK-Taktiken, die der Bedrohungsakteur in einer Angriffssequenz versucht. GuardDuty verwendet das MITRE ATT&ACK-Framework, das der gesamten Angriffssequenz Kontext hinzufügt. Die Farben, die die GuardDuty Konsole verwendet, um die Bedrohungszwecke zu spezifizieren, die vom Bedrohungsakteur verwendet wurden, entsprechen den Farben, die die Werte „Kritisch“, „Hoch“, „Mittel“ und „Niedrig“ angeben. Schweregrad der Ergebnisse

Netzwerkindikatoren

Zu den Indikatoren gehört eine Kombination von Netzwerkindikatorwerten, die erklären, warum ein Netzwerk auf ein verdächtiges Verhalten hinweist. Dieser Abschnitt gilt nur, wenn der Indikator `SUSPICIOUS_NETWORK` oder `MALICIOUS_IP` enthält. Das folgende Beispiel zeigt, wie Netzwerkindikatoren mit einem Indikator verknüpft werden könnten, wobei:

- *`AnyCompany`*ist ein Autonomes System (AS).
- `TUNNEL_VPNIS_ANONYMOUS`, und `ALLOWS_FREE_ACCESS` sind die Netzwerkindikatoren.

```
...{
    "key": "SUSPICIOUS_NETWORK",
    "values": [{
        "AnyCompany": [
            "TUNNEL_VPN",
            "IS_ANONYMOUS",
            "ALLOWS_FREE_ACCESS"
        ]
    }]
}
...
```

Die folgende Tabelle enthält die Werte der Netzwerkindikatoren und ihre Beschreibung. Diese Tags werden auf der Grundlage der Bedrohungsinformationen hinzugefügt, die aus Quellen wie Spur GuardDuty gesammelt wurden

Wert des Netzwerkanzeigers	Description
TUNNEL_VPN	Die Netzwerk- oder IP-Adresse ist einem VPN-Tunneltyp zugeordnet. Dies bezieht sich auf ein bestimmtes Protokoll, mit dessen Hilfe eine sichere, verschlüsselte Verbindung zwischen zwei Punkten über ein öffentliches Netzwerk hergestellt werden kann.
TUNNEL_PROXY	Die Netzwerk- oder IP-Adresse ist einem Proxy-Tunneltyp zugeordnet. Dies bezieht sich auf ein bestimmtes Protokoll, das beim Herstellen einer Verbindung über einen Proxyserver hilft.
TUNNEL_RDP	Die Netzwerk- oder IP-Adresse steht im Zusammenhang mit der Verwendung einer Methode zur Kapselung des Remotedesktopverkehrs (RDP) in einem anderen Protokoll, um die Sicherheit zu erhöhen, Netzwerkeinschränkungen zu umgehen oder den Fernzugriff über Firewalls zu ermöglichen.
IS_ANONYMOUS	Die Netzwerk- oder IP-Adresse ist einem bekannten anonymen Dienst oder einem Proxydienst zugeordnet. Dies kann auf potenzielle verdächtige Aktivitäten hinweisen, die sich hinter anonymen Netzwerken verstecken.

Wert des Netzwerkanzeigers	Description
KNOWN_THREAT_OPERATOR	Die Netzwerk- oder IP-Adresse ist mit einem bekanntermaßen riskanten Tunnelanbieter verknüpft. Dies weist darauf hin, dass verdächtige Aktivitäten von einer IP-Adresse aus erkannt wurden, die mit einem VPN, Proxy oder anderen Tunneldiensten verknüpft ist, die häufig für böswillige Zwecke verwendet werden.
ALLOWS_FREE_ACCESS	Die Netzwerk- oder IP-Adresse ist einem Tunnelbetreiber zugeordnet, der den Zugriff auf seinen Dienst ermöglicht, ohne dass eine Authentifizierung oder Zahlung erforderlich ist. Dazu können auch Testkonten oder eingeschränkte Nutzungserlebnisse gehören, die von verschiedenen Onlinediensten angeboten werden.
ALLOWS_CRYPTO	Die Netzwerk- oder IP-Adresse ist mit einem Tunnelanbieter (wie einem VPN oder einem Proxydienst) verknüpft, der ausschließlich Kryptowährung oder andere digitale Währungen als Zahlungsmethode akzeptiert.
ALLOWS_TORRENTS	Die Netzwerk- oder IP-Adresse ist mit Diensten oder Plattformen verknüpft, die Torrent-Verkehr zulassen. Solche Dienste werden häufig mit der Unterstützung und Nutzung von Torrents sowie mit Aktivitäten zur Umgehung von Urheberrechten in Verbindung gebracht.
RISK_CALLBACK_PROXY	Die Netzwerk- oder IP-Adresse wird Geräten zugeordnet, von denen bekannt ist, dass sie Datenverkehr an private Proxys, Malware-Proxys oder andere Callback-Proxy-Netzwerke weiterleiten. Dies bedeutet nicht, dass alle Aktivitäten im Netzwerk proxybezogen sind, sondern dass das Netzwerk in der Lage ist, den Datenverkehr im Namen dieser Proxynetzwerke weiterzuleiten.

Wert des Netzwerkanzeigers	Description
RISK_GEO_MISMATCH	Dieser Indikator deutet darauf hin, dass das Rechenzentrum oder der Hosting-Standort eines Netzwerks vom erwarteten Standort der Benutzer und Geräte dahinter abweicht. Wenn dieser Indikatorwert nicht vorhanden ist, bedeutet dies nicht, dass keine Diskrepanz vorliegt. Dies könnte bedeuten, dass nicht genügend Daten vorliegen, um die Diskrepanz zu bestätigen.
IS_SCANNER	Die Netzwerk- oder IP-Adresse steht im Zusammenhang mit permanenten Anmeldeversuchen über Webformulare.
RISK_WEB_SCRAPING	Das IP-Netzwerk ist mit automatisierten Webclients und anderen programmatischen Webaktivitäten verknüpft.
CLIENT_BEHAVIOR_FILE_SHARING	Die Netzwerk- oder IP-Adresse ist mit dem Verhalten des Clients verknüpft, das auf Filesharing-Aktivitäten wie Peer-to-Peer-Netzwerke (P2P) oder Filesharing-Protokolle hinweist.
CATEGORY_COMMERCIAL_VPN	Die Netzwerk- oder IP-Adresse ist einem Tunnelbetreiber zugeordnet, der als herkömmlicher VPN-Dienst (Commercial Virtual Private Network) eingestuft wird, der im Rechenzentrum betrieben wird.
CATEGORY_FREE_VPN	Die Netzwerk- oder IP-Adresse ist einem Tunnelbetreiber zugeordnet, der als völlig kostenloser VPN-Dienst eingestuft ist.
CATEGORY_RESIDENTIAL_PROXY	Die Netzwerk- oder IP-Adresse ist einem Tunneloperator zugeordnet, der als SDK-, Schadsoftware- oder Proxydienst mit kostenpflichtigen Quellen eingestuft ist.
OPERATOR_XXX	Der Name des Dienstanbieters, der diesen Tunnel betreibt.

Benutzerdetails für die RDS-Datenbank (DB)

> **Note**
>
> Dieser Abschnitt bezieht sich auf Ergebnisse, die bei der Aktivierung der RDS-Schutzfunktion in festgestellt wurden GuardDuty. Weitere Informationen finden Sie unter GuardDuty RDS-Schutz.

Das GuardDuty Ergebnis liefert die folgenden Benutzer- und Authentifizierungsdetails der potenziell gefährdeten Datenbank:

- Benutzer – Der Benutzername, der für den anomalen Anmeldeversuch verwendet wurde.
- Anwendung – Der Anwendungsname, der für den anomalen Anmeldeversuch verwendet wurde.
- Datenbank – Der Name der Datenbank-Instance, die an dem anomalen Anmeldeversuch beteiligt war.
- SSL – Die für das Netzwerk verwendete Version von Secure Socket Layer (SSL).
- Authentifizierungsmethode – Die Authentifizierungsmethode, die von dem Benutzer verwendet wurde, der an der Erkenntnis beteiligt war.

Hinweise zu der potenziell gefährdeten Ressource finden Sie unter. Ressource

Details zu den Erkenntnissen der Laufzeitüberwachung

> **Note**
>
> Diese Details sind möglicherweise nur verfügbar, wenn eine der GuardDuty Findetypen für die Laufzeitüberwachung folgenden GuardDuty generiert wird.

Dieser Abschnitt enthält die Laufzeitdetails wie Prozessdetails und den erforderlichen Kontext. Prozessdetails beschreiben Informationen über den beobachteten Prozess, und der Laufzeitkontext beschreibt alle zusätzlichen Informationen über die potenziell verdächtige Aktivität.

Details zum Prozess

- Name – Der Name des Prozesses.

- Ausführbarer Pfad – Absoluter Pfad der ausführbaren Zieldatei des Prozesses.
- Ausführbar SHA-256 — Der `SHA256` Hash der ausführbaren Datei des Prozesses.
- Namespace-PID – Die Prozess-ID des Prozesses in einem sekundären PID-Namespace, bei dem es sich nicht um den PID-Namespace auf Host-Ebene handelt. Bei Prozessen innerhalb eines Containers ist dies die Prozess-ID, die innerhalb des Containers beobachtet wird.
- Derzeitiges Arbeitsverzeichnis – Das aktuelle Arbeitsverzeichnis des Prozesses.
- Prozess-ID – Die ID, die dem Prozess vom Betriebssystem zugewiesen wurde.
- Startzeit – Die Uhrzeit, zu der der Prozess gestartet wurde. Dieses Feld hat das UTC-Datums-Zeichenfolgenformat (`2023-03-22T19:37:20.168Z`).
- UUID — Die eindeutige ID, die dem Prozess von zugewiesen wurde. GuardDuty
- Parent UUID – Die eindeutige ID des übergeordneten Prozesses. Diese ID wird dem übergeordneten Prozess von zugewiesen. GuardDuty
- Benutzername – Der Benutzername, der den Prozess ausgeführt hat.
- Benutzer-ID – Die Benutzer-ID des Benutzers, der den Prozess ausgeführt hat.
- Effektive Benutzer-ID – Die effektive Benutzer-ID des Prozesses zum Zeitpunkt des Ereignisses.
- Herkunft – Informationen über die Vorfahren des Prozesses.
  - Prozess-ID – Die ID, die dem Prozess vom Betriebssystem zugewiesen wurde.
  - UUID — Die eindeutige ID, die dem Prozess von zugewiesen wurde. GuardDuty
  - Ausführbarer Pfad – Absoluter Pfad der ausführbaren Zieldatei des Prozesses.
  - Effektive Benutzer-ID – Die effektive Benutzer-ID des Prozesses zum Zeitpunkt des Ereignisses.
  - Parent UUID – Die eindeutige ID des übergeordneten Prozesses. Diese ID wird dem übergeordneten Prozess von zugewiesen. GuardDuty
  - Startzeit – Die Uhrzeit, zu der der Prozess gestartet wurde.
  - Namespace-PID – Die Prozess-ID des Prozesses in einem sekundären PID-Namespace, bei dem es sich nicht um den PID-Namespace auf Host-Ebene handelt. Bei Prozessen innerhalb eines Containers ist dies die Prozess-ID, die innerhalb des Containers beobachtet wird.
  - Benutzer-ID – Die Benutzer-ID des Benutzers, der den Prozess ausgeführt hat.
  - Name – Der Name des Prozesses.

Laufzeitkontext

Aus den folgenden Feldern kann eine generierte Erkenntnis nur die Felder enthalten, die für den Erkenntnistyp relevant sind.

- Mount-Quelle – Der Pfad auf dem Host, der vom Container bereitgestellt wird.
- Mount-Ziel – Der Pfad im Container, der dem Host-Verzeichnis zugeordnet ist.
- Dateisystem-Typ – Stellt den Typ des eingehängten Dateisystems dar.
- Flags – Stellt Optionen dar, die das Verhalten des Ereignisses steuern, das an dieser Erkenntnis beteiligt ist.
- Verändernder Prozess – Informationen über den Prozess, der zur Laufzeit eine Binärdatei, ein Skript oder eine Bibliothek in einem Container erstellt oder geändert hat.
- Geändert am – Der Zeitstempel, zu dem der Prozess zur Laufzeit eine Binärdatei, ein Skript oder eine Bibliothek in einem Container erstellt oder geändert hat. Dieses Feld hat das UTC-Datums-Zeichenfolgenformat (`2023-03-22T19:37:20.168Z`).
- Bibliothekspfad – Der Pfad zur neuen Bibliothek, die geladen wurde.
- LD-Vorladungs-Wert – Der Wert der `LD_PRELOAD`-Umgebungsvariable.
- Socket-Pfad – Der Pfad zum Docker-Socket, auf den zugegriffen wurde.
- Runc-Binär-Pfad – Der Pfad zur `runc`-Binärdatei.
- Release-Agent-Pfad – Der Pfad zur `cgroup`-Release-Agent-Datei.
- Beispiel für eine Befehlszeile — Das Beispiel für die Befehlszeile, die an der potenziell verdächtigen Aktivität beteiligt war.
- Werkzeugkategorie — Kategorie, zu der das Tool gehört. Einige der Beispiele sind Backdoor Tool, Pentest Tool, Network Scanner und Network Sniffer.
- Toolname — Der Name des potenziell gefährlichen Tools.
- Dateioperation — Die Art der Dateioperation, die den Fund ausgelöst hat, wie Schreiben, Löschen, Umbenennen, Verknüpfen oder Symlink.
- Dateipfad — Der Pfad der vertraulichen Datei, die geändert wurde. Die Änderung umfasst Schreib-, Lösch-, Umbenennungs-, Link- oder Symlink-Operationen.
- Verwandte Dateipfade — Alle Dateipfade, die durch denselben Prozess geändert wurden, der die Suche ausgelöst hat, bis zu einem Maximum von 25 Pfaden.
- Skriptpfad — Der Pfad zu dem ausgeführten Skript, das den Befund generiert hat.
- Pfad der Bedrohungsdatei — Der verdächtige Pfad, für den die Bedrohungsinformationen gefunden wurden.
- Dienstname — Der Name des Sicherheitsdienstes, der deaktiviert wurde.
- Modulname — Der Name des Moduls, das in den Kernel geladen wird.

- Module SHA256 — Der SHA256-Hash des Moduls.
- Moduldateipfad — Der Pfad zu dem in den Kernel geladenen Modul.

Scan-Details der EBS-Volumes

> **Note**
>
> Dieser Abschnitt bezieht sich auf Ergebnisse, die beim Einschalten des GuardDuty-initiated Malware-Scans festgestellt wurdenMalware-Schutz für EC2.

Der EBS-Volume-Scan liefert Details über das EBS-Volume, das an die potenziell kompromittierte EC2-Instance oder den Container-Workload angehängt ist.

- Scan-ID – Die Kennung des Malware-Scans.
- Scan gestartet am – Das Datum und die Uhrzeit, zu der der Malware-Scan gestartet wurde.
- Scan abgeschlossen am – Das Datum und die Uhrzeit, zu der der Malware-Scan abgeschlossen wurde.
- Trigger Finding ID — Die Finde-ID des GuardDuty Fundes, das diesen Malware-Scan ausgelöst hat.
- Quellen — Die möglichen Werte sind `Bitdefender` und`Amazon`.

  Weitere Informationen zur Scan-Engine, die zur Erkennung von Malware verwendet wird, finden Sie unterGuardDuty Scan-Engine zur Malware-Erkennung.
- Scan-Erkennungen – Die vollständige Ansicht der Details und Ergebnisse jedes Malware-Scans.
  - Anzahl gescannter Objekte – Die Gesamtzahl der gescannten Dateien. Liefert Details wie `totalGb`, `files` und `volumes`.
  - Anzahl der entdeckten Bedrohungen – Die Gesamtzahl der während des Scans erkannten schädlichen `files`.
  - Bedrohungsdetails mit dem höchsten Schweregrad – Die Details der Bedrohung mit dem höchsten Schweregrad, die während des Scans erkannt wurde, und die Anzahl der schädlichen Dateien. Liefert Details wie `severity`, `threatName` und `count`.
  - Nach Namen erkannte Bedrohungen – Das Container-Element, in dem Bedrohungen aller Schweregrade gruppiert werden. Liefert Details wie `itemCount`, `uniqueThreatNameCount`, `shortened` und `threatNames`.

Einzelheiten zur Suche nach Malware Protection for EC2

> **Note**
>
> Dieser Abschnitt bezieht sich auf Ergebnisse, die beim Einschalten des GuardDuty-initiated Malware-Scans festgestellt wurden. Malware-Schutz für EC2

Wenn der Scan von Malware Protection for EC2 Malware erkennt, können Sie die Scandetails anzeigen, indem Sie auf der Seite Ergebnisse in der https://console.aws.amazon.com/guardduty/Konsole den entsprechenden Befund auswählen. Der Schweregrad Ihrer Entdeckung durch Malware Protection for EC2 hängt vom Schweregrad der GuardDuty Entdeckung ab.

Die folgenden Informationen sind im Abschnitt Entdeckte Bedrohungen im Detailbereich verfügbar.

- Name – Der Name der Bedrohung, der durch Gruppierung der Dateien nach Entdeckung ermittelt wurde.
- Schweregrad – Der Schweregrad der erkannten Bedrohung.
- Hash — Der SHA-256 der Datei.
- Dateipfad – Der Speicherort der schädlichen Datei auf dem EBS-Volume.
- Dateiname – Der Name der Datei, in der die Bedrohung erkannt wurde.
- Volume-ARN – Der ARN der gescannten EBS-Volumes.

Die folgenden Informationen sind im Abschnitt Malware-Scan-Details im Detailbereich verfügbar.

- Scan-ID – Die Kennung des Malware-Scans.
- Scan gestartet am – Das Datum und die Uhrzeit, zu der der Malware-Scan gestartet wurde.
- Scan abgeschlossen am – Das Datum und die Uhrzeit, zu der der Scan abgeschlossen wurde.
- Gescannte Dateien – Die Gesamtzahl der gescannten Dateien und Verzeichnisse.
- Gescannte GB insgesamt – Die Menge an Speicherplatz, die während des Vorgangs gescannt wurde.
- Erkennungs-ID des Auslösers — Die Finde-ID des GuardDuty Fundes, das diesen Malware-Scan ausgelöst hat.
- Die folgenden Informationen sind im Abschnitt Volume-Details im Detailbereich verfügbar.
  - Volume-ARN – Der Amazon-Ressourcenname (ARN) des Volumes.

- Snapshot-ARN – Der ARN des Snapshots des EBS-Volumes.
- Status – Der Scan-Status des Volumes, z. B. `Running`, `Skipped` und `Completed`.
- Verschlüsselungstyp – Der Verschlüsselungstyp, der zur Verschlüsselung des Volumes verwendet wird. Beispiel, `CMCMK`.
- Gerätename – Der Name des Geräts. Beispiel, `/dev/xvda`.

Einzelheiten zu Erkenntnissen von Malware Protection für S3

Die folgenden Informationen zum Malware-Scan sind verfügbar, wenn Sie GuardDuty sowohl als auch Malware Protection for S3 in Ihrem aktivieren AWS-Konto:

- Bedrohungen — Eine Liste der Bedrohungen, die während des Malware-Scans erkannt wurden.

> **Mehrere potenzielle Bedrohungen in Archivdateien**
>
> Wenn Sie über eine Archivdatei verfügen, die potenziell mehrere Bedrohungen enthält, meldet Malware Protection for S3 nur die erste erkannte Bedrohung. Danach wird der Scanstatus als abgeschlossen markiert. GuardDuty generiert den zugehörigen Befundtyp und sendet auch die von ihm generierten EventBridge Ereignisse. Weitere Informationen zur Überwachung der Amazon S3 S3-Objektscans mithilfe der EventBridge Ereignisse finden Sie im Beispiel-Benachrichtigungsschema für THREATS_FOUND unter. Ergebnis des S3-Objektscans

- Elementpfad — Eine Liste der verschachtelten Elementpfade und Hash-Details des gescannten S3-Objekts.
  - Verschachtelter Elementpfad — Elementpfad des gescannten S3-Objekts, in dem die Bedrohung erkannt wurde.

    Der Wert dieses Felds ist nur verfügbar, wenn es sich bei dem Objekt der obersten Ebene um ein Archiv handelt und wenn in einem Archiv eine Bedrohung erkannt wurde.
  - Hash — Der Hash der Bedrohung, die in diesem Ergebnis erkannt wurde.

> **Note**
>
> In Fällen, in denen der Hash nicht berechnet werden kann, wird das Scanergebnis trotzdem geliefert und der Hashwert ist standardmäßig auf eine leere Zeichenfolge

(`e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855`) eingestellt. SHA-256

- Quellen — Die möglichen Werte sind `Bitdefender` und`Amazon`.

  Weitere Informationen zur Scan-Engine, die zur Erkennung von Malware verwendet wird, finden Sie unterGuardDuty Scan-Engine zur Malware-Erkennung.

Action

Die Aktion einer Erkenntnis gibt Details über die Art der Aktivität, durch die das Ergebnis ausgelöst wurde. Die verfügbaren Informationen variieren je nach Aktionstyp.

Aktionstyp – Der Aktivitätstyp der Erkenntnis. Dieser Wert kann NETWORK_CONNECTION, PORT_PROBE, DNS_REQUEST oder RDS_LOGIN_ATTEMPT sein. AWS_API_CALL Die verfügbaren Informationen variieren je nach Aktionstyp:

- NETWORK_CONNECTION – Gibt an, dass Netzwerkdatenverkehr zwischen der identifizierten EC2-Instance und dem Remote-Host ausgetauscht wurde. Dieser Aktionstyp enthält die folgenden zusätzlichen Informationen:
  - Verbindungsrichtung — Die Netzwerkverbindungsrichtung, die bei der Aktivität beobachtet wurde, die zur Generierung des Ergebnisses geführt hat. GuardDuty Bei ihnen kann es sich um einen der folgenden Werte handeln:
    - INBOUND – Gibt an, dass ein Remote-Host eine Verbindung mit einem lokalen Port auf der in Ihrem Konto identifizierten EC2-Instance initiiert hat.
    - OUTBOUND – Gibt an, dass die identifizierte EC2-Instance eine Verbindung mit einem Remote-Host initiiert hat.
    - UNBEKANNT — Zeigt an, dass die Richtung der Verbindung nicht bestimmt werden GuardDuty konnte.
  - Protokoll — Das Netzwerkverbindungsprotokoll, das bei der Aktivität beobachtet wurde, die GuardDuty zur Generierung des Ergebnisses geführt hat.
  - Lokale IP – Die ursprüngliche Quell-IP-Adresse des Datenverkehrs, der die Erkenntnis ausgelöst hat. Diese Informationen können verwendet werden, um zwischen der IP-Adresse einer Zwischenebene, durch die Datenverkehr fließt, und der ursprünglichen Quell-IP-Adresse des Datenverkehrs , der die Suche ausgelöst hat, zu unterscheiden. Zum Beispiel die IP-Adresse

eines EKS-Pods im Gegensatz zur IP-Adresse der Instance, auf der der EKS-Pod ausgeführt wird.

- Blockiert – Gibt an, ob der Ziel-Port blockiert ist.

- PORT_PROBE – Gibt an, dass ein Remote-Host die identifizierte EC2-Instance auf mehreren offenen Ports untersucht hat. Dieser Aktionstyp enthält die folgenden zusätzlichen Informationen:
  - Lokale IP – Die ursprüngliche Quell-IP-Adresse des Datenverkehrs, der die Erkenntnis ausgelöst hat. Diese Informationen können verwendet werden, um zwischen der IP-Adresse einer Zwischenebene, durch die Datenverkehr fließt, und der ursprünglichen Quell-IP-Adresse des Datenverkehrs , der die Suche ausgelöst hat, zu unterscheiden. Zum Beispiel die IP-Adresse eines EKS-Pods im Gegensatz zur IP-Adresse der Instance, auf der der EKS-Pod ausgeführt wird.
  - Blockiert – Gibt an, ob der Ziel-Port blockiert ist.
- DNS_REQUEST – Gibt an, dass die identifizierte EC2-Instance einen Domainnamen abgefragt hat. Dieser Aktionstyp enthält die folgenden zusätzlichen Informationen:
  - Protokoll — Das Netzwerkverbindungsprotokoll, das bei der Aktivität beobachtet wurde, die GuardDuty zur Generierung des Ergebnisses führte.
  - Blockiert – Gibt an, ob der Ziel-Port blockiert ist.
- AWS_API_CALL— Zeigt an, dass eine AWS API aufgerufen wurde. Dieser Aktionstyp enthält die folgenden zusätzlichen Informationen:
  - API — Der Name des API-Vorgangs, der aufgerufen und somit GuardDuty zur Generierung dieses Ergebnisses aufgefordert wurde.

    > **Note**
    >
    > Diese Vorgänge können auch Nicht-API-Ereignisse einschließen, die von AWS CloudTrail erfasst wurden. Weitere Informationen finden Sie unter Non-API Ereignisse, die von CloudTrail erfasst wurden.

  - Benutzeragent – Der Benutzeragent, der die API-Anfrage gestellt hat. Dieser Wert gibt an, ob der Anruf von AWS-Managementkonsole, einem AWS Dienst, den AWS SDKs oder dem AWS CLI getätigt wurde.
  - ERROR_CODE – Wenn die Erkenntnis durch einen fehlgeschlagenen API-Aufruf ausgelöst wurde, wird der Fehlercode für diesen Aufruf angezeigt.
  - Service-Name – Der DNS-Name des Services, der versucht hat, den API-Aufruf durchzuführen, durch den die Erkenntnis ausgelöst wurde.

- RDS_LOGIN_ATTEMPT – Zeigt an, dass von einer Remote-IP-Adresse aus ein Anmeldeversuch bei der potenziell kompromittierte Datenbank unternommen wurde.
  - IP-Adresse – Die Remote-IP-Adresse, die für den potenziell verdächtigen Anmeldeversuch verwendet wurde.

Akteur oder Ziel

Eine Erkenntnis verfügt über den Abschnitt Actor, wenn die Ressourcenrolle `TARGET` war. Dies zeigt an, dass verdächtige Aktivitäten auf Ihre Ressource ausgerichtet waren, und der Abschnitt Actor enthält Details zur Entität, von der diese auf Ihre Ressource ausgerichtet wurden.

Eine Erkenntnis hat einen Ziel-Abschnitt, wenn die Ressourcenrolle `ACTOR` lautete. Dies zeigt an, dass Ihre Ressource an verdächtigen Aktivitäten gegen einen Remote-Host beteiligt war. Dieser Abschnitt enthält Informationen zur IP-Adresse und/oder Domain, auf die Ihre Ressource ausgerichtet ist.

Im Abschnitt Actor oder Ziel können folgende Informationen verfügbar sein:

- Verbunden — Details darüber, ob das AWS Konto des Remote-API-Aufrufers mit Ihrer GuardDuty Umgebung verknüpft ist. Wenn dieser Wert `true` ist, ist der API-Aufrufer in irgendeiner Weise Ihrem Konto zugeordnet. Falls der Wert `false` ist, stammt der API-Aufrufer von außerhalb Ihrer Umgebung.
- Remote-Konto-ID — Die Konto-ID, der die ausgehende IP-Adresse gehört, die für den Zugriff auf die Ressource im endgültigen Netzwerk verwendet wurde.
- IP-Adresse — Die IP-Adresse, die an der Aktivität beteiligt war, die GuardDuty zur Generierung des Ergebnisses geführt hat.
- Standort — Standortinformationen für die IP-Adresse, die an der Aktivität beteiligt war, die GuardDuty zur Generierung des Ergebnisses geführt hat.
- Organisation — Informationen zur ISP-Organisation der IP-Adresse, die an der Aktivität beteiligt war, die GuardDuty zur Generierung des Ergebnisses geführt hat.
- Port — Die Portnummer, die an der Aktivität beteiligt war, die GuardDuty zur Generierung des Ergebnisses geführt hat.
- Domain — Die Domain, die an der Aktivität beteiligt war, die GuardDuty zur Generierung des Ergebnisses geführt hat.

- Domain mit Suffix — Die Domain der zweiten und obersten Ebene, die an einer Aktivität beteiligt war, die möglicherweise GuardDuty zur Generierung des Ergebnisses geführt hat. Eine Liste der Domänen der obersten und zweiten Ebene finden Sie in der Liste der öffentlichen Suffixe.

Einzelheiten zur Geolokalisierung

GuardDuty bestimmt den Standort und das Netzwerk von Anfragen mithilfe von MaxMind GeoIP-Datenbanken. MaxMind meldet eine sehr hohe Genauigkeit ihrer Daten auf Landesebene, obwohl die Genauigkeit je nach Faktoren wie Land und Art der IP-Adresse variiert.

Weitere Informationen MaxMind dazu finden Sie unter MaxMind IP-Geolokalisierung. Wenn Sie der Meinung sind, dass einige der GeoIP-Daten falsch sind, senden Sie eine Korrekturanfrage MaxMind an MaxMindCorrect GeoIP2 Data.

Zusätzliche Informationen

Alle Erkenntnisse verfügen über einen Abschnitt Zusätzliche Informationen, der die folgenden Informationen enthalten kann:

- Name der Bedrohungsliste — Der Name der Bedrohungsliste, die die IP-Adresse oder den Domainnamen enthält, der an der Aktivität beteiligt war, die GuardDuty zur Generierung des Fundes geführt hat.
- Beispiel – Der Wert Wahr oder Falsch, gibt an, ob es sich um ein Beispiel-Erkenntnis handelt.
- Archiviert – Der Wert Wahr oder Falsch, gibt an, ob diese Erkenntnis archiviert wurde.
- Ungewöhnlich – Aktivitätsdetails, die zuvor noch nicht beobachtet wurden. Dabei kann es sich um ungewöhnliche (zuvor nicht beobachtete) Benutzer, Standorte, Zeitpunkte, Buckets, Anmeldeverhalten oder ASN Org handeln.
- Ungewöhnliches Protokoll — Das Netzwerkverbindungsprotokoll, das an der Aktivität beteiligt war, die GuardDuty zur Generierung des Befundes geführt hat.
- Agentendetails – Details über den Sicherheitsagent, der derzeit auf dem EKS-Cluster in Ihrem AWS-Konto installiert ist. Dies gilt nur für Erkenntnistypen von der EKS-Laufzeit-Überwachung.
  - Agent-Version — Die Version des GuardDuty Security Agents.
  - Agenten-ID — Die eindeutige Kennung des GuardDuty Security Agents.

Beweise

Erkenntnisse, die auf Bedrohungsinformationen basieren, haben einen Abschnitt Beweise, der die folgenden Informationen enthält:

- Informationen zur Bedrohungsinformation — Der Name der Bedrohungsliste, auf der die erkannte Bedrohung aufgeführt `Threat name` ist.
- Name der Bedrohung — Der Name der Malware-Familie oder eine andere Kennung, die mit der Bedrohung verknüpft ist.
- Bedrohungsdatei SHA256 — SHA256 der Datei, die den Befund generiert hat.

Anormales Verhalten

Arten von Ergebnissen, die auf enden, AnomalousBehaviorweisen darauf hin, dass der Befund durch das ML-Modell (Machine Learning) zur Erkennung von GuardDuty Anomalien generiert wurde. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Taktiken von Angreifern in Verbindung gebracht werden. Das ML-Modell verfolgt verschiedene Faktoren der API-Anfrage, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und die spezifische API, die angefordert wurde.

Einzelheiten darüber, welche Faktoren der API-Anfrage für die CloudTrail Benutzeridentität, die die Anfrage aufgerufen hat, ungewöhnlich sind, finden Sie in den Ergebnisdetails. Die Identitäten werden durch das CloudTrail UserIdentity-Element definiert, und die möglichen Werte sind:`Root`,,, `IAMUserAssumedRole`, `FederatedUser` oder. `AWSAccount` `AWSService`

Zusätzlich zu den Informationen, die für alle GuardDuty Ergebnisse im Zusammenhang mit API-Aktivitäten verfügbar sind, enthalten die AnomalousBehaviorErgebnisse zusätzliche Details, die im folgenden Abschnitt beschrieben werden. Diese Details können in der Konsole eingesehen werden und sind auch in der JSON-Datei des Erkenntnisses verfügbar.

- Anomale APIs – Eine Liste von API-Anfragen, die von der Benutzeridentität in der Nähe der mit der Erkenntnis verknüpften primären API-Anfrage aufgerufen wurden. In diesem Bereich werden die Details des API-Erkenntnisses wie folgt weiter aufgeschlüsselt.
  - Bei der ersten aufgeführten API handelt es sich um die primäre API, d. h. um die API-Anfrage, die mit der beobachteten Aktivität mit dem höchsten Risiko verknüpft ist. Dies ist die API, welche die Erkenntnis ausgelöst hat und mit der Angriffsphase des Erkenntnistyps korreliert. Dies ist

auch die API, die im Abschnitt Aktion in der Konsole und in der JSON-Datei des Erkenntnisses detailliert beschrieben wird.

- Bei allen anderen aufgeführten APIs handelt es sich um zusätzliche anomale APIs, die anhand der aufgelisteten Benutzeridentität in der Nähe der primären API beobachtet wurden. Wenn nur eine API auf der Liste steht, hat das ML-Modell keine zusätzlichen API-Anfragen von dieser Benutzeridentität als anomal identifiziert.
- Die Liste der APIs ist danach unterteilt, ob eine API erfolgreich aufgerufen wurde oder ob die API erfolglos aufgerufen wurde, was bedeutet, dass eine Fehlerantwort empfangen wurde. Die Art der empfangenen Fehlerantwort ist über jeder API aufgeführt, die erfolglos aufgerufen wurde. Mögliche Fehlerantworttypen sind: `access denied`, `access denied exception`, `auth failure`, `instance limit exceeded`, `invalid permission - duplicate`, `invalid permission - not found` und `operation not permitted`.
- APIs werden nach dem zugehörigen Service kategorisiert.
- Wenn Sie mehr Kontext benötigen, wählen Sie Historische APIs aus, um die Details zu den wichtigsten APIs (maximal 20) anzuzeigen, die normalerweise sowohl für die Benutzeridentität als auch für alle Benutzer innerhalb des Kontos angezeigt werden. Die APIs sind als Selten (weniger als einmal pro Monat), Gelegentlich (einige Male im Monat) oder Häufig (täglich bis wöchentlich) gekennzeichnet, je nachdem, wie oft sie in Ihrem Konto verwendet werden.

- Ungewöhnliches Verhalten (Konto) – In diesem Abschnitt finden Sie zusätzliche Informationen zum profilierten Verhalten Ihres Kontos.

> **Profiliertes Verhalten**
>
> GuardDuty erfährt anhand der übermittelten Ereignisse kontinuierlich mehr über die Aktivitäten in Ihrem Konto. Diese Aktivitäten und ihre beobachtete Häufigkeit werden als profiliertes Verhalten bezeichnet.

Zu den in diesem Bereich erfassten Informationen gehören:

- ASN Org — Die Organisation mit der Autonomous System Number (ASN), von der aus der anomale API-Aufruf getätigt wurde.
- Benutzername – Der Name des Benutzers, der den anomalen API-Aufruf ausgeführt hat.
- Benutzeragent – Der Benutzeragent, der für den anomalen API-Aufruf verwendet wurde. Der Benutzeragent ist die Methode, mit der der Aufruf ausgeführt wird, z. B. `aws-cli` oder `Botocore`.

  - Benutzertyp – Der Typ des Benutzers, der den anomalen API-Aufruf ausgeführt hat. Mögliche Werte sind `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER` oder `ROLE`.
  - Bucket – Der Name des S3-Buckets, auf den zugegriffen wurde.
- Ungewöhnliches Verhalten (Benutzeridentität) – Dieser Abschnitt enthält zusätzliche Informationen zum profilierten Verhalten der Benutzeridentität, die an der Erkenntnis beteiligt war. Wenn ein Verhalten nicht als historisch identifiziert wurde, bedeutet dies, dass das GuardDuty ML-Modell diese Benutzeridentität während des Trainingszeitraums noch nicht auf diese Weise aufgerufen hat. Die folgenden zusätzlichen Details zur Benutzeridentität sind verfügbar:
  - ASN Org – Die ASN-Organisation, von der aus der anomale API-Aufruf getätigt wurde.
  - Benutzeragent – Der Benutzeragent, der für den anomalen API-Aufruf verwendet wurde. Der Benutzeragent ist die Methode, mit der der Aufruf ausgeführt wird, z. B. `aws-cli` oder `Botocore`.
  - Bucket – Der Name des S3-Buckets, auf den zugegriffen wurde.
- Ungewöhnliches Verhalten (Bucket) – Dieser Abschnitt enthält zusätzliche Informationen zum profilierten Verhalten des S3-Buckets, der mit der Erkenntnis verknüpft ist. Wenn ein Verhalten nicht als historisch identifiziert wurde, bedeutet dies, dass das GuardDuty ML-Modell innerhalb des Trainingszeitraums noch keine API-Aufrufe auf diese Weise an diesen Bucket gesendet hat. Zu den in diesem Bereich erfassten Informationen gehören:
  - ASN Org – Die ASN-Organisation, von der aus der anomale API-Aufruf getätigt wurde.
  - Benutzername – Der Name des Benutzers, der den anomalen API-Aufruf ausgeführt hat.
  - Benutzeragent – Der Benutzeragent, der für den anomalen API-Aufruf verwendet wurde. Der Benutzeragent ist die Methode, mit der der Aufruf ausgeführt wird, z. B. `aws-cli` oder `Botocore`.
  - Benutzertyp – Der Typ des Benutzers, der den anomalen API-Aufruf ausgeführt hat. Mögliche Werte sind `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER` oder `ROLE`.

> **Note**
>
> Weitere Informationen zu historischen Verhaltensweisen finden Sie unter Historisches Verhalten in den Abschnitten Ungewöhnliches Verhalten (Konto), Benutzer-ID oder Bucket, wo Sie Details zum erwarteten Verhalten in Ihrem Konto für jede der folgenden Kategorien anzeigen können: Selten (weniger als einmal pro Monat), Gelegentlich (einige Male pro Monat) oder Häufig (täglich bis wöchentlich), je nachdem, wie oft sie in Ihrem Konto verwendet werden.

- Ungewöhnliches Verhalten (Datenbank) – Dieser Abschnitt enthält zusätzliche Informationen zum profilierten Verhalten der Datenbank-Instance, das mit der Erkenntnis verknüpft ist. Wenn ein Verhalten nicht als historisch identifiziert wurde, bedeutet dies, dass das GuardDuty ML-Modell innerhalb des Trainingszeitraums noch keinen Anmeldeversuch auf diese Weise bei dieser Datenbankinstanz festgestellt hat. Zu den Informationen, die für diesen Abschnitt im Erkenntnisbereich verfolgt werden, gehören:
  - Benutzer – Der Benutzername, der für den anomalen Anmeldeversuch verwendet wurde.
  - ASN Org – Die ASN-Organisation, von der aus der anomale API-Aufruf getätigt wurde.
  - Anwendung – Der Anwendungsname, der für den anomalen Anmeldeversuch verwendet wurde.
  - Datenbank – Der Name der Datenbank-Instance, die an dem anomalen Anmeldeversuch beteiligt war.

  Der Abschnitt Historisches Verhalten bietet mehr Kontext zu den zuvor beobachteten Benutzernamen, ASN-Organisationen, Anwendungsnamen und Datenbanknamen für die zugehörige Datenbank. Jedem Einzelwert ist eine Anzahl zugeordnet, die angibt, wie oft dieser Wert bei einer erfolgreichen Anmeldung beobachtet wurde.
- Ungewöhnliches Verhalten (Konto-Kubernetes-Cluster, Kubernetes-Namespace und Kubernetes-Benutzername) – In diesem Abschnitt finden Sie zusätzliche Informationen zum profilierten Verhalten des Kubernetes-Clusters und des mit der Erkenntnis verbundenen Namespaces. Wenn ein Verhalten nicht als historisch identifiziert wird, bedeutet dies, dass das GuardDuty ML-Modell diesen Account, Cluster, Namespace oder Benutzernamen zuvor nicht auf diese Weise beobachtet hat. Zu den Informationen, die für diesen Abschnitt im Erkenntnisbereich verfolgt werden, gehören:
  - Benutzername – Der Benutzer, der die der Erkenntnis zugeordnete Kubernetes-API aufgerufen hat.
  - Impersonierter Nutzername – Der Benutzer, für den sich `username` ausgibt.
  - Namespace – Der Kubernetes-Namespace innerhalb des Amazon-EKS-Clusters, in dem die Aktion stattgefunden hat.
  - Benutzeragent – Der Benutzeragent, der dem Kubernetes-API-Aufruf zugeordnet ist. Der Benutzeragent ist die Methode, mit der der Aufruf ausgeführt wird, z. B. `kubectl`.
  - API – Die Kubernetes-API, die von `username` innerhalb des Amazon-EKS-Clusters aufgerufen wird.
  - ASN-Informationen – Die ASN-Informationen, wie Organisation und ISP, die der IP-Adresse des Benutzers zugeordnet sind, der diesen Aufruf tätigt.
  - Wochentag – Der Wochentag, an dem der Kubernetes-API-Aufruf getätigt wurde.

- Permission — Das Kubernetes-Verb und die Ressource, die auf Zugriff geprüft werden, geben an, ob sie die Kubernetes-API verwenden `username` können oder nicht.
- Dienstkontoname — Das dem Kubernetes-Workload zugeordnete Dienstkonto, das dem Workload eine Identität verleiht.
- Registrierung — Die Container-Registry, die dem Container-Image zugeordnet ist, das im Kubernetes-Workload bereitgestellt wird.
- Image — Das Container-Image ohne die zugehörigen Tags und Digest, das im Kubernetes-Workload bereitgestellt wird.
- Image-Präfix-Konfiguration — Das Image-Präfix mit aktivierter Container- und Workload-Sicherheitskonfiguration, z. B. `hostNetwork` oder`privileged`, für den Container, der das Image verwendet.
- Betreffname — Die Subjekte, wie z. B. a `usergroup`, oder, `serviceAccountName` die an eine Referenzrolle in einem `RoleBinding` oder gebunden sind`ClusterRoleBinding`.
- Rollenname — Der Name der Rolle, die an der Erstellung oder Änderung von Rollen oder der `roleBinding` API beteiligt ist.

Volumenbezogene S3-Anomalien

In diesem Abschnitt werden die Kontextinformationen für volumenbasierte S3-Anomalien detailliert beschrieben. Die volumenbasierte Erkenntnis (Exfiltration:S3/AnomalousBehavior) überwacht, ob Benutzer ungewöhnlich viele S3-API-Aufrufe an die S3-Buckets tätigen, was auf eine mögliche Datenexfiltration hindeutet. Die folgenden S3-API-Aufrufe werden im Hinblick auf die volumenbasierte Erkennung von Anomalien überwacht.

- `GetObject`
- `CopyObject.Read`
- `SelectObjectContent`

Die folgenden Metriken würden dabei helfen, eine Grundlage für das übliche Verhalten zu schaffen, wenn eine IAM-Entität auf einen S3-Bucket zugreift. Um Datenexfiltration zu erkennen, werden bei der volumenbasierten Erkennung von Anomalien alle Aktivitäten anhand der üblichen Verhaltensgrundlagen bewertet. Wählen Sie die Option Historisches Verhalten in den Abschnitten Ungewöhnliches Verhalten (Benutzeridentität), Beobachtetes Volumen (Benutzeridentität) und Beobachtetes Volumen (Bucket) aus, um jeweils die folgenden Metriken anzuzeigen.

- Anzahl der `s3-api-name`-API-Aufrufe, die von dem IAM-Benutzer oder der IAM-Rolle (je nachdem, welche ausgestellt wurde), der/die dem betroffenen S3-Bucket zugeordnet ist, in den letzten 24 Stunden durchgeführt wurden.
- Anzahl der `s3-api-name`-API-Aufrufe, die vom IAM-Benutzer oder von der IAM-Rolle (je nachdem, welche ausgestellt wurde) der/die allen S3-Buckets zugeordnet ist, in den letzen 24 Stunden durchgeführt wurden.
- Anzahl der `s3-api-name`-API-Aufrufe über alle IAM-Benutzer oder IAM-Rollen (je nachdem, welche ausgestellt wurden), die dem betroffenen S3-Bucket zugeordnet sind, in den letzten 24 Stunden durchgeführt wurden.

Anomalien aufgrund von RDS-Anmeldeaktivitäten

In diesem Abschnitt wird die Anzahl der Anmeldeversuche des ungewöhnlichen Akteurs detailliert beschrieben und nach den Ergebnissen der Anmeldeversuche gruppiert. Die Erkenntnistypen für RDS Protection identifizieren anomales Verhalten, indem sie die Anmeldeereignisse auf ungewöhnliche Muster von `successfulLoginCount`, `failedLoginCount` und `incompleteConnectionCount` überwachen.

- erfolgreich LoginCount — Dieser Zähler stellt die Summe der erfolgreichen Verbindungen (richtige Kombination von Anmeldeattributen) dar, die der ungewöhnliche Akteur mit der Datenbankinstanz hergestellt hat. Zu den Anmeldeattributen gehören Benutzername, Passwort und Datenbankname.
- fehlgeschlagen LoginCount — Dieser Zähler stellt die Summe der fehlgeschlagenen (erfolglosen) Anmeldeversuche dar, die unternommen wurden, um eine Verbindung zur Datenbank-Instance herzustellen. Dies weist darauf hin, dass ein oder mehrere Attribute der Anmeldekombination, wie Benutzername, Passwort oder Datenbankname, falsch waren.
- unvollständig ConnectionCount — Dieser Zähler stellt die Anzahl der Verbindungsversuche dar, die nicht als erfolgreich oder fehlgeschlagen eingestuft werden können. Diese Verbindungen werden geschlossen, bevor die Datenbank eine Antwort liefert. Beispielsweise Port-Scanning, bei dem der Datenbank-Port zwar verbunden ist, aber keine Information an die Datenbank gesendet wird, oder die Verbindung vor Abschluss der Anmeldung entweder erfolgreich oder fehlgeschlagen abgebrochen wurde.

GuardDuty Aggregation finden

GuardDuty aktualisiert die generierten Ergebnisse dynamisch. Wenn eine neue Aktivität im Zusammenhang mit demselben Sicherheitsproblem GuardDuty entdeckt wird, GuardDuty wird das

ursprüngliche Ergebnis mit den neuesten Details aktualisiert, anstatt ein neues Ergebnis zu erstellen. Dieses Verhalten ermöglicht es Ihnen, alle laufenden Probleme zu identifizieren, ohne mehrere ähnliche Berichte durchsehen zu müssen, und reduziert das Gesamtvolumen der Funde bekannter Sicherheitsprobleme.

Bei der UnauthorizedAccess:EC2/SSHBruteForce Suche werden beispielsweise mehrere Zugriffsversuche auf Ihre Instance zu derselben Ergebnis-ID zusammengefasst, wodurch die Anzahl der Treffer in den Ergebnisdetails erhöht wird. Dies liegt daran, dass dieses Ergebnis ein einziges Sicherheitsproblem darstellt, wobei die Instance anzeigt, dass der SSH-Port auf der Instance nicht ordnungsgemäß vor dieser Art von Aktivität geschützt ist. Wenn GuardDuty jedoch SSH-Zugriffsaktivitäten für eine neue Instance in Ihrer Umgebung erkennt, wird ein neues Ergebnis mit einer eindeutigen Ergebniskennung erstellt, die Sie darauf hinzuweisen, dass mit der neuen Ressource ein Sicherheitsproblem verbunden ist.

Wenn ein Ergebnis aggregiert wird, wird es mit Informationen aus dem letzten Auftreten dieser Aktivität aktualisiert. Das bedeutet, dass im obigen Beispiel, wenn Ihre Instance das Ziel eines Brute-Force-Versuchs von einem neuen Akteur ist, die Erkenntnisdetails aktualisiert werden, um die Remote-IP der jüngsten Quelle wiederzugeben, und ältere Informationen ersetzt werden. Vollständige Informationen über einzelne Aktivitätsversuche sind weiterhin in Ihren CloudTrail Protokollen oder VPC Flow Logs verfügbar.

Die Kriterien, anhand derer GuardDuty Sie ein neues Ergebnis generieren, anstatt ein vorhandenes zu aggregieren, hängen vom Typ des Ergebnisses ab. Die Aggregationskriterien für jeden Ergebnistyp werden von unseren Sicherheitstechnikern festgelegt, um einen Überblick über die verschiedenen Sicherheitsprobleme in Ihrem Konto zu erhalten.

Wenn in Ihrem Konto ein Erkennungstyp für eine Angriffssequenz GuardDuty generiert wird, wird das Ergebnis nur dann aggregiert, wenn Sie ähnliche Signale in derselben Reihenfolge in Ihrem Konto GuardDuty identifizieren. Andernfalls GuardDuty wird eine weitere Angriffssequenz generiert.

Verwaltung der GuardDuty Amazon-Ergebnisse

GuardDuty bietet mehrere wichtige Funktionen, mit denen Sie Ihre Ergebnisse sortieren, speichern und verwalten können. Diese Funktionen helfen Ihnen dabei, die Ergebnisse auf Ihre spezifische Umgebung zuzuschneiden, das Rauschen aufgrund von Ergebnissen mit geringem Wert zu reduzieren und sich auf Bedrohungen für Ihre individuelle AWS Umgebung zu konzentrieren. Lesen Sie die Themen auf dieser Seite, um zu erfahren, wie Sie diese Funktionen nutzen können, um den Wert von Sicherheitsergebnissen in Ihrer Umgebung zu erhöhen.

Themen:

[Übersichts-Dashboard in Amazon GuardDuty](#)

Erfahren Sie mehr über die Komponenten des Übersichts-Dashboards, das in der GuardDuty Konsole verfügbar ist.

[Ergebnisse filtern in GuardDuty](#)

Erfahren Sie, wie Sie GuardDuty Ergebnisse anhand der von Ihnen angegebenen Kriterien filtern können.

[Unterdrückungsregeln in GuardDuty](#)

Erfahren Sie, wie Sie mithilfe von Unterdrückungsregeln die Ergebnisse, auf die Sie GuardDuty aufmerksam gemacht werden, automatisch filtern können. Mithilfe von Unterdrückungsregeln werden Erkenntnisse automatisch auf der Grundlage von Filtern archiviert.

[Anpassen der Bedrohungserkennung mit Entitätenlisten und IP-Adresslisten](#)

Passen Sie den Umfang der GuardDuty Überwachung mithilfe von IP-Listen und Bedrohungslisten an, die auf öffentlich routingfähigen IP-Adressen basieren. Vertrauenswürdige IP-Listen verhindern, dass aus IP-Adressen, die Sie für vertrauenswürdig halten, Ergebnisse generiert werden, die nichts mit DNS GuardDuty zu tun haben, während Intel-Bedrohungslisten Sie vor Aktivitäten von benutzerdefinierten IP-Adressen warnen.

[Generierte Ergebnisse nach Amazon S3 exportieren](#)

Exportieren Sie die generierten Ergebnisse in einen Amazon S3 S3-Bucket, sodass Sie Aufzeichnungen auch nach Ablauf der 90-tägigen Aufbewahrungsfrist für Ergebnisse verwalten können. GuardDuty Verwenden Sie diese historischen Daten, um potenzielle

verdächtige Aktivitäten in Ihrem Konto nachzuverfolgen und zu bewerten, ob die empfohlenen Abhilfemaßnahmen erfolgreich waren.

Bearbeitung von GuardDuty Ergebnissen mit Amazon EventBridge

Richten Sie automatische Benachrichtigungen für GuardDuty Ergebnisse im Rahmen von EventBridge Amazon-Veranstaltungen ein. Sie können auch andere Aufgaben automatisieren EventBridge , um auf Ergebnisse zu reagieren.

Grundlegendes zu CloudWatch Protokollen und Gründen für das Überspringen von Ressourcen beim Scan von Malware Protection for EC2

Erfahren Sie, wie Sie die CloudWatch Logs for GuardDuty Malware Protection for EC2 überprüfen können und aus welchen Gründen Ihre betroffenen Amazon EC2 EC2-Instance- oder Amazon EBS-Volumes während des Scanvorgangs möglicherweise übersprungen wurden.

Falschmeldungen in Malware Protection for EC2 melden

Erfahren Sie, wie Sie potenzielle falsch positive Bedrohungserkennungen in Malware Protection for EC2 melden können.

S3-Objektscanergebnis in Malware Protection for S3 als falsch positiv melden

Erfahren Sie, wie Sie potenzielle falsch positive Bedrohungserkennungen in Malware Protection for S3 melden können.

Falschmeldungen in Malware Protection for Backup melden

Erfahren Sie, wie Sie potenzielle falsch positive Bedrohungserkennungen in Malware Protection for Backup melden können.

Übersichts-Dashboard in Amazon GuardDuty

Das GuardDuty Übersichts-Dashboard bietet eine aggregierte Ansicht der GuardDuty Ergebnisse, die AWS-Konto in Ihrer aktuellen AWS-Region Version generiert wurden.

Wenn Sie ein GuardDuty Administratorkonto verwenden, bietet das Dashboard aggregierte Statistiken und Daten für Ihr Konto und Ihre Mitgliedskonten in Ihrer Organisation.

Übersichts-Dashboard anzeigen

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   GuardDuty zeigt standardmäßig das Übersichts-Dashboard an, wenn Sie die Konsole öffnen.

2. Wählen Sie auf der Übersichtsseite in der Regionsauswahl oben rechts in der Konsole die gewünschte Option AWS-Region aus.
3. Wählen Sie im Auswahlmenü für den Zeitraum den Zeitraum aus, für den Sie die Zusammenfassung anzeigen möchten. Standardmäßig zeigt das Dashboard die Daten für den heutigen Tag, den heutigen Tag, an.

> **Note**
>
> Wenn im ausgewählten Zeitraum keine Ergebnisse generiert wurden, enthält das Dashboard keine Daten zur Anzeige. Sie können das Dashboard aktualisieren oder den Datumsbereich anpassen.

Themen

- -Übersicht
- Ergebnisse
- Die häufigsten Arten von Erkenntnissen
- Erkenntnisse nach Schweregrad
- Konten mit den meisten Erkenntnissen
- Ressourcen mit Erkenntnissen
- Am wenigsten auftretende Erkenntnisse
- Geltungsbereich der Schutzpläne

-Übersicht

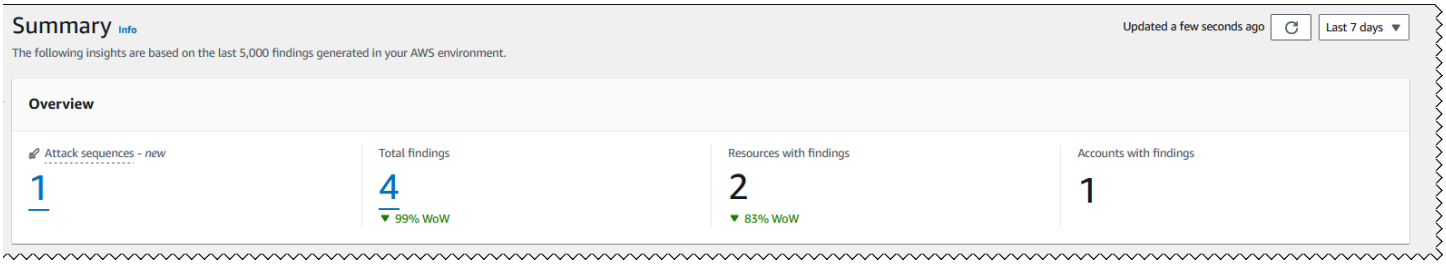
Diese Einstellung bietet die folgenden Optionen:

- Angriffssequenzen: Gibt die Anzahl der Ergebnisse der Angriffssequenz an, die in Ihrem Konto in der aktuellen Region GuardDuty generiert wurden.

  GuardDuty erkennt potenzielle mehrstufige Angriffe auf Ihr Konto. Sie können die Nummer unter Angriffssequenzen auswählen, um die Details auf der Seite Ergebnisse einzusehen.
- Erkenntnisse insgesamt: Gibt die Gesamtzahl von Erkenntnissen an, die in Ihrem Konto in der aktuellen Region generiert wurden. Dies umfasst sowohl einzelne Ergebnisse als auch Ergebnisse der Angriffssequenz.

- Ressourcen mit Ergebnissen: Gibt die Anzahl der Ressourcen an, die mit einem Ergebnis verknüpft sind und potenziell gefährdet wurden.
- Konten mit Erkenntnissen: Gibt die Anzahl der Konten an, in denen mindestens eine Erkenntnis generiert wurde. Wenn Sie ein eigenständiges Konto haben, ist der Wert in diesem Feld 1.

Für die Zeitbereiche Letzte 7 Tage und Letzte 30 Tage kann im Bereich Übersicht der prozentuale Unterschied zwischen den generierten Erkenntnissen von Woche zu Woche (WoW) bzw. Monat zu Monat (MoM) angezeigt werden. Wenn in der Woche oder im Monat zuvor keine Erkenntnisse generiert wurden und keine Vergleichsdaten vorliegen, ist die prozentuale Differenz möglicherweise nicht verfügbar.



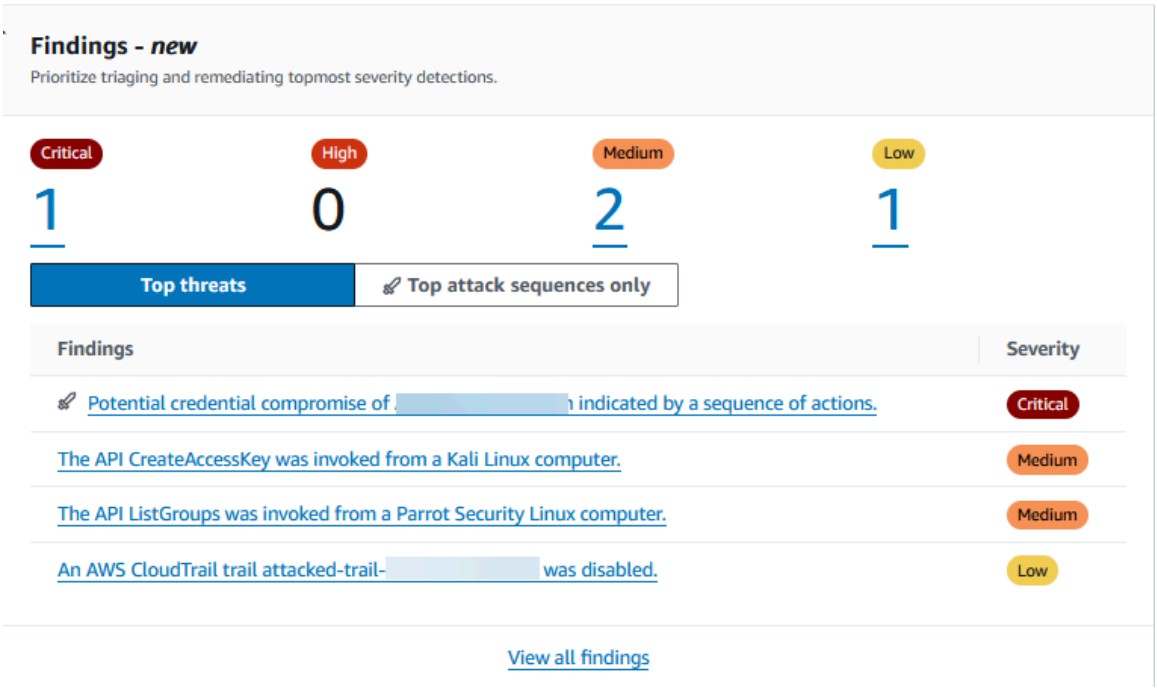
Wenn Sie ein GuardDuty Administratorkonto haben, enthalten all diese Felder die zusammengefassten Daten aller Mitgliedskonten in Ihrer Organisation.

Ergebnisse

Das Ergebnis-Widget zeigt bis zu acht Top-Ergebnisse an. Diese Ergebnisse werden nach ihrem Schweregrad aufgelistet, wobei Kritische Ergebnisse zuerst angezeigt werden.

Standardmäßig können Sie alle Ergebnisse anzeigen. Um nur Daten zu Ergebnissen der Angriffssequenz anzuzeigen, aktivieren Sie „Nur Top-Angriffssequenzen“.

In dieser Liste können Sie ein beliebiges Ergebnis auswählen, um dessen Details anzuzeigen.



Die häufigsten Arten von Erkenntnissen

Dieser Abschnitt enthält ein Kreisdiagramm, das die fünf häufigsten Ergebnisarten veranschaulicht, die in der aktuellen Region generiert wurden. Wenn Sie den Mauszeiger über die einzelnen Sektoren des Kreisdiagramms bewegen, können Sie Folgendes beobachten:

- Anzahl der Ergebnisse: Gibt an, wie oft dieses Ergebnis im ausgewählten Zeitraum generiert wurde.
- Schweregrad: Gibt den Schweregrad des Ergebnisses an.
- Prozentsatz: Gibt den Anteil dieses Ergebnistyps im Verhältnis zum Gesamtwert an.
- Zuletzt generiert: Gibt an, wie viel Zeit vergangen ist, seit dieser Befundtyp zuletzt erkannt wurde.

Erkenntnisse nach Schweregrad

In diesem Abschnitt wird ein Balkendiagramm angezeigt, das die Gesamtzahl der Ergebnisse im ausgewählten Zeitraum anzeigt. Das Diagramm unterteilt die Ergebnisse nach Schweregrad (Kritisch, Hoch, Mittel und Niedrig) und hilft Ihnen dabei, die Anzahl der Ergebnisse für bestimmte Daten innerhalb des Bereichs anzuzeigen.

Um die Anzahl für jeden Schweregrad an einem bestimmten Datum anzuzeigen, bewegen Sie den Mauszeiger über den entsprechenden Balken im Diagramm.

Konten mit den meisten Erkenntnissen

Diese Einstellung bietet die folgenden Optionen:

- Konto: Gibt die AWS-Konto ID an, unter der das Ergebnis generiert wurde.
- Anzahl der Erkenntnisse: Gibt an, wie oft eine Erkenntnis für diese Konto-ID generiert wurde.
- Zuletzt generiert: Gibt an, wie viel Zeit seit der letzten Generierung dieses Erkenntnistyps vergangen ist.
- Filter für Schweregrad: Standardmäßig werden die Daten für die Arten von Ergebnissen mit hohem Schweregrad angezeigt. Mögliche Optionen für dieses Feld sind Gesamter Schweregrad, Kritischer Schweregrad, Hoher Schweregrad und Mittlerer Schweregrad.

Ressourcen mit Erkenntnissen

Diese Einstellung bietet die folgenden Optionen:

- Ressource: Zeigt den potenziell betroffenen Ressourcentyp an. Wenn diese Ressource zu Ihrem Konto gehört, können Sie auf den Quicklink zugreifen, um die Ressourcendetails einzusehen. Wenn Sie ein GuardDuty Administratorkonto haben, können Sie die Details der potenziell betroffenen Ressource einsehen, indem Sie mit den Anmeldeinformationen des Besitzer-Mitgliedskontos auf die GuardDuty Konsole zugreifen.
- Konto: Gibt die AWS-Konto ID an, zu der diese Ressource gehört.
- Anzahl der Erkenntnisse: Gibt an, wie oft diese Ressource mit einer Erkenntnis verknüpft wurde.
- Zuletzt generiert: Gibt an, wie viel Zeit seit der letzten Generierung dieses Erkenntnistyps vergangen ist.
- Ressourcentypfilter: Standardmäßig werden die Daten für alle Ressourcentypen angezeigt. Mithilfe dieses Filters können Sie wählen, ob Sie die Daten für einen bestimmten Ressourcentyp wie Instance AccessKey, Lambda und andere anzeigen möchten.
- Schweregradfilter: Standardmäßig werden die Daten für „Gesamter Schweregrad“ angezeigt. Mithilfe dieses Filters können Sie wählen, ob Sie die Daten für andere Schweregrade anzeigen möchten. Mögliche Optionen sind Kritischer Schweregrad, Hoher Schweregrad, Mittlerer Schweregrad und Gesamter Schweregrad.

Am wenigsten auftretende Erkenntnisse

In diesem Abschnitt wird das Auffinden von Typen beschrieben, die in Ihrer AWS Umgebung selten vorkommen. Dieses Widget soll Ihnen helfen, potenzielle neu auftretende Bedrohungsmuster zu identifizieren und zu untersuchen.

Dieses Widget zeigt die folgenden Daten an:

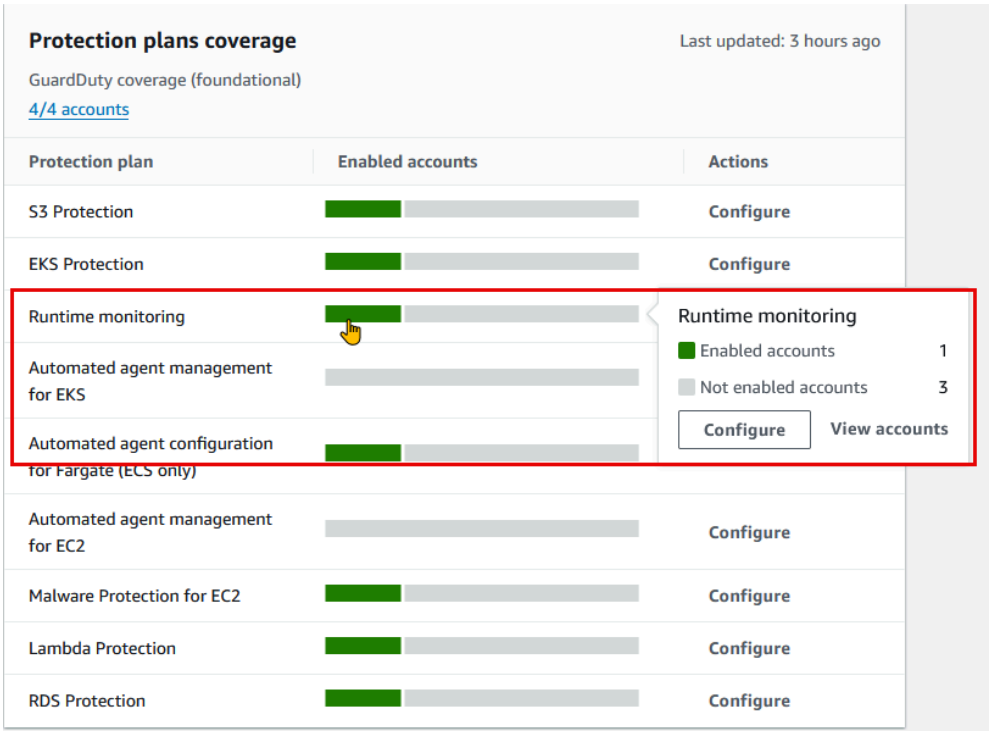
- Suchtyp: Zeigt den Namen des Suchtyps an.
- Anzahl der Erkenntnisse: Gibt an, wie oft diese Erkenntnis im ausgewählten Zeitraum generiert wurde.
- Zuletzt generiert: Gibt an, wie viel Zeit seit der letzten Generierung dieses Erkenntnistyps vergangen ist.
- Filter für Schweregrad: Standardmäßig werden die Daten für die Typen mit hohem Schweregrad angezeigt. Mögliche Optionen für dieses Feld sind Kritischer Schweregrad, Hoher Schweregrad, Mittlerer Schweregrad und Gesamter Schweregrad.

Geltungsbereich der Schutzpläne

In diesem Abschnitt werden Statistiken für die Mitgliedskonten in Ihrer Organisation angezeigt. Er zeigt die Anzahl der Mitgliedskonten, die in der aktuellen Region aktiviert wurden GuardDuty (grundlegende Bedrohungserkennung). Nur ein delegierter GuardDuty Administrator kann die Statistiken für die Mitgliedskonten innerhalb seiner Organisation einsehen. Wenn Sie eine neue AWS Organisation erstellen, kann es bis zu 24 Stunden dauern, bis die Statistiken für die gesamte Organisation generiert sind.

Wie benutzt man dieses Widget

- Konfiguration: Wenn kein Schutzplan konfiguriert ist, wählen Sie in der Spalte Aktionen die Option Konfigurieren aus.
- Aktivierte Konten anzeigen: Bewegen Sie den Mauszeiger über die Leiste in der Spalte Aktivierte Konten, um zu sehen, für wie viele Konten die einzelnen Schutzpläne aktiviert wurden. Um weitere Kontodetails einzusehen, klicken Sie auf den grünen Balken und wählen Sie Konten anzeigen aus.



Ergebnisse filtern in GuardDuty

Mit einem Erkenntnisfilter können Sie Erkenntnisse anzeigen, die den von Ihnen angegebenen Kriterien entsprechen, und alle nicht übereinstimmenden Erkenntnisse herausfiltern. Sie können Suchfilter ganz einfach mit der GuardDuty Amazon-Konsole oder mit der CreateFilterAPI mithilfe von JSON erstellen. Lesen Sie die folgenden Abschnitte, um zu erfahren, wie Sie einen Filter in der Konsole erstellen. Informationen zur Verwendung dieser Filter zur automatischen Archivierung eingehender Erkenntnisse finden Sie unter Unterdrückungsregeln in GuardDuty.

Beachten Sie bei der Erstellung von Filtern die folgende Liste:

- Sie können mindestens ein Attribut oder maximal 50 Attribute als Kriterien für einen bestimmten Filter angeben.
- Wenn Sie den Operator „Gleich“ oder „Entspricht nicht“ verwenden, um nach einem Attributwert wie der Konto-ID zu filtern, können Sie maximal 50 Werte angeben.
- Jedes Filterkriterienattribut wird als AND-Operator ausgewertet. Mehrere Werte für dasselbe Attribut werden als AND/OR ausgewertet.
- Informationen zur maximalen Anzahl von gespeicherten Filtern, die Sie AWS-Konto in jedem Filter erstellen können AWS-Region, finden Sie unter. GuardDuty Kontingente

- Die Felder unter `service.additionalInfo` werden mit ihrem vollständigen JSON-Pfad angegeben, genau wie jedes andere Feld. Beispiel: `{ "service.additionalInfo.sample": { "Equals": ["true"] } }`.
- Timestamp-Felder akzeptieren Werte im Millisekundenformat von Unix Epoch (z. B.). `1486685375000` Eine vollständige Liste der Timestamp-Felder finden Sie in der Anmerkung unten.

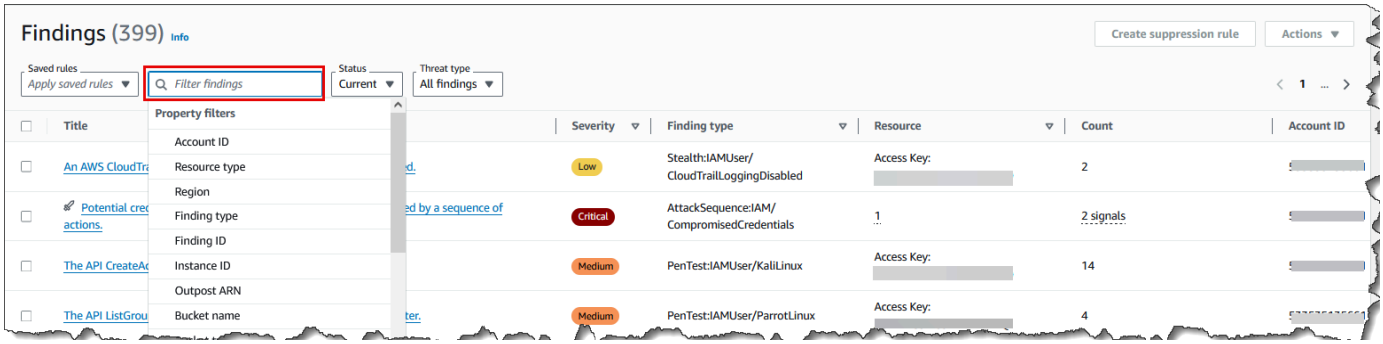
Die folgenden Abschnitte enthalten Anweisungen zum Erstellen und Speichern von Filtern mithilfe von GuardDuty Konsolen-, API- und CLI-Befehlen. Wählen Sie Ihre bevorzugte Zugriffsmethode, um fortzufahren.

Filtersatz in der GuardDuty Konsole erstellen und speichern

Suchfilter können über die GuardDuty Konsole erstellt und getestet werden. Sie können über die Konsole erstellte Filter speichern, um sie in Unterdrückungsregeln oder zukünftigen Filtervorgängen zu verwenden. Ein Filter besteht aus mindestens einem Filterkriterium, das aus einem Filterattribut in Kombination mit mindestens einem Wert besteht.

Um Filterkriterien zu erstellen und zu speichern (Konsole)

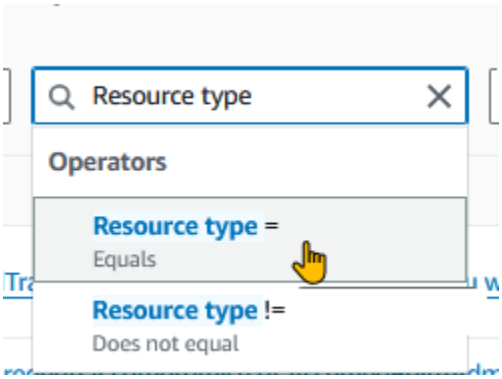
1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im linken Navigationsbereich Findings aus.
3. Wählen Sie auf der Seite Ergebnisse die Leiste Ergebnisse filtern neben dem Menü Gespeicherte Regeln aus. Daraufhin wird eine erweiterte Liste von Eigenschaftenfiltern angezeigt.



4. Wählen Sie aus der erweiterten Filterliste ein Attribut aus, auf dessen Grundlage Sie die Ergebnistabelle filtern möchten.

Um beispielsweise Ergebnisse anzuzeigen, bei denen es sich bei der potenziell betroffenen Ressource um einen S3-Bucket handelt, wählen Sie Ressourcentyp aus.

5. Wählen Sie für Operatoren einen Operator aus, der Ihnen hilft, die Ergebnisse zu filtern, um das gewünschte Ergebnis zu erzielen. Um mit dem Beispiel aus dem vorherigen Schritt fortzufahren, wählen Sie Ressourcentyp =. Daraufhin wird eine Liste der Ressourcentypen in angezeigt GuardDuty.



Wenn Ihr Anwendungsfall das Ausschließen bestimmter Ergebnisse erfordert, können Sie „Entspricht nicht“ oder „!“ wählen. = Operator.

6. Geben Sie den Wert für den ausgewählten Eigenschaftenfilter an. Wählen Sie bei Bedarf Anwenden aus. Um mit dem Beispiel aus dem vorherigen Schritt fortzufahren, können Sie S3Bucket wählen.

   Dadurch werden die Ergebnisse angezeigt, die mit den angewendeten Filtern übereinstimmen.

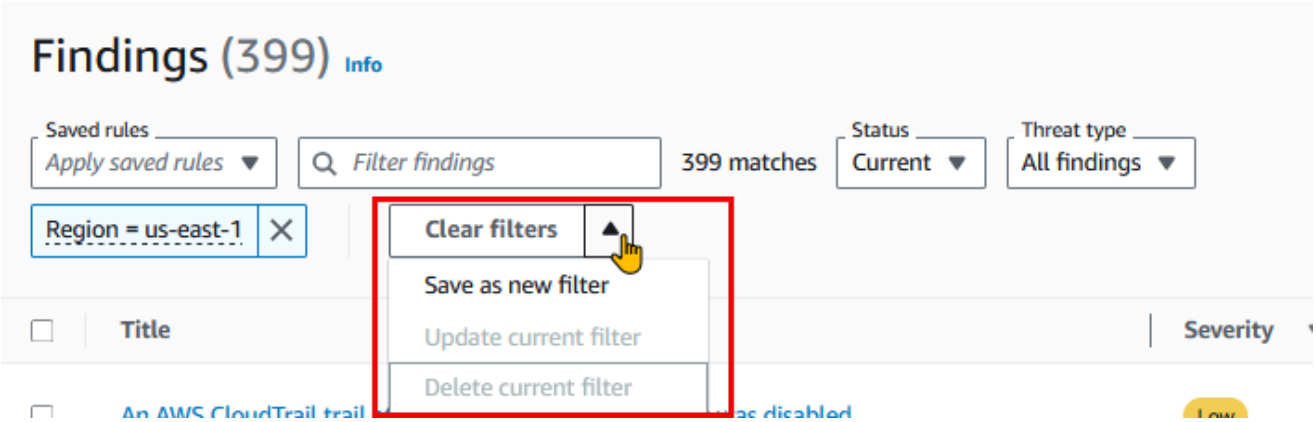
7. Um mehr als ein Filterkriterium hinzuzufügen, wiederholen Sie die Schritte 3-6.

   Eine vollständige Liste der Attribute finden Sie unterEigenschaftsfilter in GuardDuty.

8. (Optional) Speichern Sie die angegebenen Attribute und Werte als Filter

   Um diese Filterkombination in future erneut anzuwenden, können Sie die angegebenen Attribute und ihre Werte als Filtersatz speichern.

   a. Nachdem Sie ein Filterkriterium mit einem oder mehreren Eigenschaftsfiltern erstellt haben, wählen Sie den Pfeil im Menü Filter löschen aus.



b. Geben Sie den Namen des Filtersatzes ein. Der Name muss 3-64 Zeichen lang sein. Gültige Zeichen sind a-z A-Z, 0-9, Punkt (.), Bindestrich (-) und Unterstrich (_).

c. Die Beschreibung ist optional. Wenn Sie eine Beschreibung eingeben, kann diese bis zu 512 Zeichen enthalten.

d. Wählen Sie Erstellen aus.

Filtersatz mithilfe von GuardDuty API und CLI erstellen und speichern

Sie können die Suchfilter entweder mithilfe von API- oder CLI-Befehlen erstellen und testen. Ein Filter besteht aus mindestens einem Filterkriterium, das aus einem Filterattribut in Kombination mit mindestens einem Wert besteht. Sie können Filter speichern, um sie später zu erstellen Unterdrückungsregeln oder andere Filtervorgänge auszuführen.

Um Suchfilter zu erstellen mit API/CLI

- Führen Sie die CreateFilterAPI aus, indem Sie die regionale Detektor-ID des AWS-Konto Standorts verwenden, für den Sie einen Filter erstellen möchten.

  Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

- Alternativ können Sie die Create-Filter-CLI verwenden, um den Filter zu erstellen und zu speichern. Sie können ein oder mehrere Filterkriterien von verwenden. Eigenschaftsfilter in GuardDuty

  Verwenden Sie die folgenden Beispiele, indem Sie die rot markierten Platzhalterwerte ersetzen.

Beispiel 1: Erstellen Sie einen neuen Filter, um alle Ergebnisse anzuzeigen, die einem bestimmten Befundtyp entsprechen

Im folgenden Beispiel wird ein Filter erstellt, der allen `PortScan` Ergebnissen für eine Instanz entspricht, die aus einem bestimmten Bild erstellt wurde. Die Platzhalterwerte werden rot angezeigt. Ersetzen Sie diese Werte durch geeignete Werte für Ihr Konto. Ersetzen Sie sie beispielsweise *12abc34d567e8fa901bc2d34EXAMPLE* durch Ihre regionale Melder-ID.

```
aws guardduty create-filter \
--detector-id 12abc34d567e8fa901bc2d34EXAMPLE \
--name FilterExampleName \
--finding-criteria '{"Criterion": {"type": {"Equals": ["Recon:EC2/Portscan"]},
 "resource.instanceDetails.imageId": {"Equals":["ami-0a7a207083example"]}} }'
```

Beispiel 2: Erstellen Sie einen neuen Filter, um alle Ergebnisse anzuzeigen, die den Schweregraden entsprechen

Im folgenden Beispiel wird ein Filter erstellt, der allen Ergebnissen entspricht, die mit den `HIGH` Schweregraden verknüpft sind. Die Platzhalterwerte werden rot dargestellt. Ersetzen Sie diese Werte durch geeignete Werte für Ihr Konto. Ersetzen Sie sie beispielsweise *12abc34d567e8fa901bc2d34EXAMPLE* durch Ihre regionale Melder-ID.

```
aws guardduty create-filter \
--detector-id 12abc34d567e8fa901bc2d34EXAMPLE \
--name FilterExampleName \
--finding-criteria '{"Criterion": {"severity": {"Equals": ["7", "8"]}} }'
```

- Denn API/CLI sie Schweregrad der Ergebnisse werden als Zahlen dargestellt. Verwenden Sie die folgenden Werte, um die Ergebnisse nach Schweregrad zu filtern:
  - Verwenden Sie für `LOW` Schweregrade `{ "severity": { "Equals": ["1", "2", "3"] } }`
  - Verwenden Sie für `MEDIUM` Schweregrade `{ "severity": { "Equals": ["4", "5", "6"] } }`
  - Verwenden Sie für `HIGH` Schweregrade `{ "severity": { "Equals": ["7", "8"] } }`
  - Verwenden Sie für `CRITICAL` Schweregrade `{ "severity": { "Equals": ["9", "10"] } }`
  - Verwenden Sie für Ergebnisse mit mehreren Schweregraden Platzhalterwerte, die dem folgenden Beispiel ähneln: `{ "severity": { "Equals": ["7", "8", "9", "10"] } }`

In diesem Beispiel werden die Ergebnisse angezeigt, die entweder einen `HIGH` oder einen `CRITICAL` Schweregrad haben.

> **Note**
>
> Wenn Sie ein Beispiel mit nur einem numerischen Wert anstelle aller numerischen Werte angeben, die einem Schweregrad zugeordnet sind, zeigen die API und die CLI möglicherweise die gefilterten Ergebnisse an. Wenn Sie diesen gespeicherten Filtersatz in der GuardDuty Konsole verwenden, funktioniert er nicht wie erwartet. Das liegt daran, dass die GuardDuty Konsole die Filterwerte als`CRITICAL`, `HIGHMEDIUM`, und betrachtet`LOW`. Beispielsweise wird von einem Filter, der mit einem CLI-Befehl erstellt wurde, der Folgendes enthält, `{ "severity": { "Equals": ["9"] } }` erwartet, dass er eine entsprechende Ausgabe in anzeigt API/CLI. Dieser gespeicherte Filter enthält jedoch bei Verwendung in der GuardDuty Konsole den Schweregrad „Teilschweregrad“ und zeigt keine erwartete Ausgabe an. Dies macht es erforderlich, dass die API und die CLI alle Werte angeben, die jedem Schweregrad zugeordnet sind.

Lebenszyklus-Metadaten filtern

Wenn Sie Filterdetails mithilfe der GetFilterAPI abrufen, können Sie Lebenszyklus-Metadatenfelder anzeigen. Diese Felder zeigen, wann ein Filter erstellt wurde und wie oft er geändert wurde.

Die GetFilter Antwort umfasst die folgenden Lebenszyklus-Metadatenfelder:

`createdAt`

Der Zeitstempel, zu dem der Filter ursprünglich erstellt wurde. GuardDuty legt diesen Wert bei der Erstellung fest und ändert ihn nie. GuardDuty füllt dieses Feld nicht für ältere Filter aus (Filter, die Sie vor dem Start dieser Funktion erstellt haben).

`updatedAt`

Der Zeitstempel, zu dem der Filter zuletzt aktualisiert wurde. GuardDuty aktualisiert diesen Wert bei jedem erfolgreichen UpdateFilterAufruf. Zum Zeitpunkt der Erstellung `updatedAt` stimmt es überein`createdAt`. Bei älteren Filtern wird dieses Feld erst angezeigt, nachdem Sie den Filter mindestens einmal aktualisiert haben.

`version`

Eine Ganzzahl, die zählt, wie oft Sie den Filter geändert haben. Sie beginnt bei der Erstellung des Filters bei 1 und wird bei jedem erfolgreichen UpdateFilter Aufruf um 1 erhöht, unabhängig davon, ob sich der Filterinhalt ändert. GuardDuty füllt dieses Feld für ältere Filter nicht aus.

> **Note**
>
> Diese Lebenszyklus-Metadatenfelder sind schreibgeschützt. Die UpdateFilter Operationen CreateFilter und akzeptieren diese Felder nicht als Eingabe, und ihre Antworten enthalten diese Felder nicht. Rufen Sie an, um Lebenszyklus-Metadaten einzusehenGetFilter.

Eigenschaftsfilter in GuardDuty

Wenn Sie Filter erstellen oder Erkenntnisse mithilfe der API-Vorgänge sortieren, müssen Sie Filterkriterien in JSON angeben. Diese Filterkriterien korrelieren mit den JSON-Details einer Erkenntnis. Die folgende Tabelle enthält eine Liste der Konsolenanzeigenamen für Filterattribute und die entsprechenden JSON-Feldnamen.

Konsolen-Feldname	JSON-Feldname
Konto-ID	accountId
Die ID des Ergebnisses	id
Region	Region
Schweregrad	severity Sie können die Befundtypen auf der Grundlage des Schweregrads der Befundtypen filtern. Weitere Informationen zu Schweregradwerten finden Sie unterSchweregrad der Ergebnisse GuardDuty. Wenn Sie `severity` zusammen mit API AWS CLI, oder verwenden CloudForm ation, wird ihr ein numerischer Wert zugewiese n. Weitere Informationen finden Sie unter

Konsolen-Feldname	JSON-Feldname
	FindingCriteria in der Amazon GuardDuty API-Referenz.
Ergebnistyp	type
Aktualisiert um	updatedAt
Access Key ID	resource.access KeyDetails.accessKeyId
Haupt-ID	resource.access KeyDetails.principalId
Username	resource.access KeyDetails.userName
Benutzertyp	resource.access KeyDetails.userType
ID des IAM-Instance-Profils	resource.instanz Details.iamInstanceProfile.id
Instance-ID	resource.instanz Details.instanceId
ID des Instance-Image	resource.instanz Details.imageId
Instance-Tag-Schlüssel	resource.instanz Details.tags.key
Instance-Tag-Wert	resource.instanz Details.tags.value
IPv6-Adresse	resource.instanz Details.networkInterfaces.ipv6Addresses
Private IPv4-Adresse	resource.instanz Details.networkInterfaces.privateIpAddresses.privateIpAddress
Öffentlicher DNS-Name	resource.instanz Details.networkInterfaces.publicDnsName
Öffentliche IP	resource.instanz Details.networkInterfaces.publicIp
Sicherheitsgruppen-ID	resource.instanz Details.networkInterfaces.securityGroups.groupId

Konsolen-Feldname	JSON-Feldname
Name der Sicherheitsgruppe	resource.instanz Details.networkInterfaces.securityGroups.groupName
Subnetz-ID	resource.instanz Details.networkInterfaces.subnetId
VPC-ID	resource.instanz Details.networkInterfaces.vpcId
Outpost-ARN	resource.instanz Details.outpostARN
Ressourcentyp	resource.resourceType
Bucket-Berechtigungen	resource.s3 BucketDetails.publicAccess.effectivePermission
Bucket-Name	ressource.s3 BucketDetails.name
Bucket-Tag-Schlüssel	ressource.s3 BucketDetails.tags.key
Bucket-Tag-Wert	ressource.s3 BucketDetails.tags.value
Bucket-Typ	ressource.s3 BucketDetails.type
Aktionstyp	service.action.actionType
Aufgerufene API	service.action.aws ApiCallAction.api
API-Aufrufertyp	service.action.aws ApiCallAction.callerType
API-Fehlercode	service.action.aws ApiCallAction.errorCode
Stadt des API-Aufrufers	service.action.aws ApiCallAction.remoteIpDetails.city.cityName
Land des API-Aufrufers	service.action.aws ApiCallAction.remoteIpDetails.country.countryName

Konsolen-Feldname	JSON-Feldname
IPv4-Adresse des API-Aufrufers	service.action.aws ApiCallAction.remoteIpDetails.ipAddressV4
IPv6-Adresse des API-Aufrufers	service.action.aws ApiCallAction.remoteIpDetails.ipAddressV6
ASN-ID des API-Aufrufers	service.action.aws ApiCallAction.remoteIpDetails.organization.asn
ASN-Name des API-Aufrufers	service.action.aws ApiCallAction.remoteIpDetails.organization.asnOrg
Servicename des API-Aufrufers	service.action.aws ApiCallAction.serviceName
DNS-Anforderungs-Domain	service.action.dns RequestAction.domain
Domainsuffix der DNS-Anforderung	service.action.dns RequestAction.domainWithSuffix
Netzwerkverbindung blockiert	service.action.network ConnectionAction.blocked
Netzwerkverbindungsrichtung	service.action.netzwerk ConnectionAction.connectionDirection
Netzwerkverbindung lokaler Port	service.action.netzwerk ConnectionAction.localPortDetails.port
Netzwerkverbindungsprotokoll	service.action.netzwerk ConnectionAction.protocol
Netzwerkverbindung Stadt	service.action.netzwerk ConnectionAction.remoteIpDetails.city.cityName
Netzwerkverbindung Land	service.action.netzwerk ConnectionAction.remoteIpDetails.country.countryName

Konsolen-Feldname	JSON-Feldname
Remote-IPv4-Adresse der Netzwerkverbindung	service.action.netzwerk ConnectionAction.remoteIpDetails.ipAddressV4
Netzwerkverbindung, Remote-IPv6-Adresse	service.action.network ConnectionAction.remoteIpDetails.ipAddressV6
Remote IP ASN-ID der Netzwerkverbindung	service.action.netzwerk ConnectionAction.remoteIpDetails.organization.asn
Remote IP ASN-Name der Netzwerkverbindung	service.action.netzwerk ConnectionAction.remoteIpDetails.organization.asnOrg
Remote-Port der Netzwerkverbindung	service.action.netzwerk ConnectionAction.remotePortDetails.port
Remote-Konto zugeordnet	service.action.aws ApiCallAction.remoteAccountDetails.affiliated
IPv4-Adresse des Kubernetes-API-Aufrufers	service.action.kubernetes ApiCallAction.remoteIpDetails.ipAddressV4
IPv6-Adresse des Kubernetes-API-Aufrufers	service.action.kubernetes ApiCallAction.remoteIpDetails.ipAddressV6
Kubernetes-Namespace	service.action.kubernetes ApiCallAction.namespace
ASN-ID des Kubernetes-API-Aufrufers	service.action.kubernetes ApiCallAction.remoteIpDetails.organization.asn
URI für die Kubernetes-API-Aufrufanforderung	service.action.kubernetes ApiCallAction.requestUri
Kubernetes-API-Statuscode	service.action.kubernetes ApiCallAction.statusCode
Lokale IPv4-Adresse der Netzwerkverbindung	service.action.netzwerk ConnectionAction.localIpDetails.ipAddressV4

Konsolen-Feldname	JSON-Feldname
Netzwerkverbindung lokale IPv6-Adresse	service.action.network ConnectionAction.localIpDetails.ipAddressV6
Protocol (Protokoll)	service.action.netzwerk ConnectionAction.protocol
Servicename des API-Aufrufs	service.action.aws ApiCallAction.serviceName
Konto-ID des API-Aufrufers	service.action.aws ApiCallAction.remoteAccountDetails.accountId
Name der Bedrohungsliste	service.zusätzlich Info.threatListName
Ressourcenrolle	service.resourceRole
EKS-Cluster-Name	resource.eks ClusterDetails.name
Name des Kubernetes-Workloads	resource.kubernetes Details.kubernetes WorkloadDetails.name
Namespace des Kubernetes-Workloads	resource.kubernetes Details.kubernetes WorkloadDetails.namespace
Kubernetes-Benutzername	resource.kubernetes Details.kubernetes UserDetails.username
Kubernetes-Container-Image	resource.kubernetes Details.kubernetes WorkloadDetails.containers.image
Kubernetes-Container-Image-Präfix	resource.kubernetes Details.kubernetes WorkloadDetails.containers.imagePrefix
Scan-ID	service.ebs VolumeScanDetails.scanId
Name der EBS-Volume-Scan-Bedrohung	service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.name

Konsolen-Feldname	JSON-Feldname
Name der Bedrohung durch S3-Objektscan	service.malware ScanDetails.threats.name
Schweregrad der Bedrohung	service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.severity
Datei-SHA	service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.filePaths.hash
ECS-Cluster-Name	resource.ecs ClusterDetails.name
ECS-Container-Image	resource.ecs ClusterDetails.taskDetails.containers.image
ARN der ECS-Aufgabendefinition	resource.ecs ClusterDetails.taskDetails.definitionArn
Eigenständiges Container-Image	resource.container Details.image
Datenbank-Instance-ID	resource.rds DbInstanceDetails.dbInstanceIdentifier
Datenbank-Cluster-ID	resource.rds DbInstanceDetails.dbClusterIdentifier
Datenbank-Engine	resource.rds DbInstanceDetails.engine
Datenbankbenutzer	resource.rds DbUserDetails.user
Ausführbar SHA-256	service.runtime Details.process.executableSha256
Prozessname	service.runtime Details.process.name
Pfad der ausführbaren Datei	service.runtime Details.process.executablePath
Lambda-Funktionsname	resource.lambda Details.functionName

Konsolen-Feldname	JSON-Feldname
ARN der Lambda-Funktion	Ressource.lambda Details.functionArn
Lambda-Funktions-Tag-Schlüssel	Ressource.lambda Details.tags.key
Tag-Wert der Lambda-Funktion	Ressource.lambda Details.tags.value
DNS-Anforderungs-Domain	service.action.dns RequestAction.domainWithSuffix

Alle anderen Suchfelder (unten aufgeführt) sind nur als Filterkriterien für Unterdrückungsregeln verfügbar (mit und). CreateFilterUpdateFilter Diese Felder werden von anderen API-Vorgängen nicht unterstützt. Unterdrückungsregeln, die diese Felder verwenden, müssen über die API erstellt oder aktualisiert werden. Diese Felder können nur für Filter mit einer `ARCHIVE` Aktion angewendet werden.

> **Note**
>
> Die folgenden Felder akzeptieren Zeitstempelwerte im Millisekundenformat der Unix-Epoche (`1262309025000`steht beispielsweise für Freitag, den 1. Januar 2010 um 01:23:45 Uhr GMT):
>
> - createdAt
> - updatedAt
> - service.event FirstSeen
> - Service.Veranstaltung LastSeen
> - resource.instanz Details.launchTime
> - resource.lambda Details.lastModifiedAt
> - resource.s3 BucketDetails.createdAt
> - resource.eks ClusterDetails.createdAt
> - resource.ecs ClusterDetails.taskDetails.createdAt
> - resource.ecs ClusterDetails.taskDetails.startedAt
> - service.ebs VolumeScanDetails.scanStartedAt
> - service.ebs VolumeScanDetails.scanCompletedAt
> - service.runtime Details.context.modifiedAt
> - service.runtime Details.context.modifyingProcess.startTime
> - service.runtime Details.context.modifyingProcess.lineage.startTime
> - service.runtime Details.context.targetProcess.startTime

- service.runtime Details.context.targetProcess.lineage.startTime
- service.runtime Details.process.startTime
- service.runtime Details.process.lineage.startTime
- service.detection.sequence.actors.session.createdTime
- service.detection.sequence.signals.CreatedAt
- service.detection.sequence.signals.updatedat
- service.detection.sequence.signals.first SeenAt
- service.detection.sequence.signals.last SeenAt
- service.detection.sequence.resources.data.s3 Bucket.createdAt
- service.detection.sequence.resources.data.ecs Task.createdAt
- service.detection.sequence.resources.data.eks Cluster.createdAt

JSON-Feldname
arn
assoziiert AttackSequenceArn
createdAt
Partition
resource.access KeyDetails.userIdentity.accessKeyId
resource.access KeyDetails.userIdentity.accountId
resource.access KeyDetails.userIdentity.arn
resource.access KeyDetails.userIdentity.principalId
resource.access KeyDetails.userIdentity.sessionContext.attributes.mfaAuthenticated
resource.access KeyDetails.userIdentity.sessionContext.ec2RoleDelivery
resource.access KeyDetails.userIdentity.sessionContext.invokedBy
resource.access KeyDetails.userIdentity.sessionContext.sessionIssuer.accountId
resource.access KeyDetails.userIdentity.sessionContext.sessionIssuer.arn

JSON-Feldname
resource.access KeyDetails.userIdentity.sessionContext.sessionIssuer.principalId
resource.access KeyDetails.userIdentity.sessionContext.sessionIssuer.type
resource.access KeyDetails.userIdentity.sessionContext.sessionIssuer.userName
resource.access KeyDetails.userIdentity.sessionContext.sourceIdentity
resource.access KeyDetails.userIdentity.sessionContext.webIdFederationData.attributes
resource.access KeyDetails.userIdentity.sessionContext.webIdFederationData.federatedProvider
resource.access KeyDetails.userIdentity.type
resource.access KeyDetails.userIdentity.userName
resource.grundgestein GuardrailDetails.guardrailArn
Ressource. Grundgestein GuardrailDetails.guardrailVersion
resource.container Details.containerRuntime
resource.container Details.imagePrefix
resource.container Details.securityContext.allowPrivilegeEscalation
resource.container Details.securityContext.privileged
resource.container Details.volumeMounts.mountPath
resource.container Details.volumeMounts.name
resource.ebs VolumeDetails.scannedVolumeDetails.deviceName
resource.ebs VolumeDetails.scannedVolumeDetails.encryptionType
resource.ebs VolumeDetails.scannedVolumeDetails.kmsKeyArn
resource.ebs VolumeDetails.scannedVolumeDetails.snapshotArn

JSON-Feldname
resource.ebs VolumeDetails.scannedVolumeDetails.volumeArn
resource.ebs VolumeDetails.scannedVolumeDetails.volumeSizeInGB
resource.ebs VolumeDetails.scannedVolumeDetails.volumeType
resource.ebs VolumeDetails.skippedVolumeDetails.deviceName
resource.ebs VolumeDetails.skippedVolumeDetails.encryptionType
resource.ebs VolumeDetails.skippedVolumeDetails.kmsKeyArn
resource.ebs VolumeDetails.skippedVolumeDetails.snapshotArn
resource.ebs VolumeDetails.skippedVolumeDetails.volumeArn
resource.ebs VolumeDetails.skippedVolumeDetails.volumeSizeInGB
resource.ebs VolumeDetails.skippedVolumeDetails.volumeType
resource.ecs ClusterDetails.activeServicesCount
resource.ecs ClusterDetails.arn
resource.ecs ClusterDetails.registeredContainerInstancesCount
resource.ecs ClusterDetails.runningTasksCount
resource.ecs ClusterDetails.status
resource.ecs ClusterDetails.tags.key
resource.ecs ClusterDetails.tags.value
resource.ecs ClusterDetails.taskDetails.arn
resource.ecs ClusterDetails.taskDetails.containers.containerRuntime
resource.ecs ClusterDetails.taskDetails.containers.id

JSON-Feldname
resource.ecs ClusterDetails.taskDetails.containers.imagePrefix
resource.ecs ClusterDetails.taskDetails.containers.name
resource.ecs ClusterDetails.taskDetails.containers.securityContext.allowPrivilegeEscalation
resource.ecs ClusterDetails.taskDetails.containers.securityContext.privileged
resource.ecs ClusterDetails.taskDetails.containers.volumeMounts.mountPath
resource.ecs ClusterDetails.taskDetails.containers.volumeMounts.name
resource.ecs ClusterDetails.taskDetails.createdAt
resource.ecs ClusterDetails.taskDetails.group
resource.ecs ClusterDetails.taskDetails.launchType
resource.ecs ClusterDetails.taskDetails.startedAt
resource.ecs ClusterDetails.taskDetails.startedBy
resource.ecs ClusterDetails.taskDetails.tags.key
resource.ecs ClusterDetails.taskDetails.tags.value
resource.ecs ClusterDetails.taskDetails.version
resource.ecs ClusterDetails.taskDetails.volumes.hostPath.path
resource.ecs ClusterDetails.taskDetails.volumes.name
resource.eks ClusterDetails.arn
resource.eks ClusterDetails.createdAt
resource.eks ClusterDetails.status
resource.eks ClusterDetails.tags.key

JSON-Feldname
resource.eks ClusterDetails.tags.value
resource.eks ClusterDetails.vpcId
resource.instance Details.iamInstanceProfile.arn
resource.instanz Details.instanceState
resource.instanz Details.instanceType
resource.instanz Details.launchTime
resource.instanz Details.networkInterfaces.networkInterfaceId
resource.instanz Details.networkInterfaces.privateDnsName
resource.instanz Details.networkInterfaces.privateIpAddress
resource.instanz Details.networkInterfaces.privateIpAddresses.privateDnsName
resource.instanz Details.platform
resource.instanz Details.productCodes.productCodeId
resource.instanz Details.productCodes.productCodeType
resource.kubernetes Details.kubernetesUserDetails.groups
resource.kubernetes Details.kubernetesUserDetails.impersonatedUser.groups
resource.kubernetes Details.kubernetesUserDetails.impersonatedUser.username
resource.kubernetes Details.kubernetesUserDetails.sessionName
resource.kubernetes Details.kubernetesUserDetails.uid
resource.kubernetes Details.kubernetesWorkloadDetails.containers.containerRuntime
resource.kubernetes Details.kubernetesWorkloadDetails.containers.id

JSON-Feldname
resource.kubernetes Details.kubernetesWorkloadDetails.containers.name
resource.kubernetes Details.kubernetesWorkloadDetails.containers.securityContext.allowPrivilegeEscalation
resource.kubernetes Details.kubernetesWorkloadDetails.containers.securityContext.privileged
resource.kubernetes Details.kubernetesWorkloadDetails.containers.volumeMounts.mountPath
resource.kubernetes Details.kubernetesWorkloadDetails.containers.volumeMounts.name
resource.kubernetes Details.kubernetesWorkloadDetails.hostIpc
resource.kubernetes Details.kubernetesWorkloadDetails.hostNetwork
resource.kubernetes Details.kubernetesWorkloadDetails.hostPid
resource.kubernetes Details.kubernetesWorkloadDetails.serviceAccountName
resource.kubernetes Details.kubernetesWorkloadDetails.type
resource.kubernetes Details.kubernetesWorkloadDetails.uid
resource.kubernetes Details.kubernetesWorkloadDetails.volumes.hostPath.path
resource.kubernetes Details.kubernetesWorkloadDetails.volumes.name
resource.lambda Details.description
Ressource.lambda Details.lastModifiedAt
Ressource.lambda Details.revisionId
Ressource.lambda Details.vpcConfig.securityGroups.groupId
Ressource.lambda Details.vpcConfig.securityGroups.groupName
Ressource.lambda Details.vpcConfig.subnetIds
Ressource.lambda Details.vpcConfig.vpcId

JSON-Feldname
resource.rds DbInstanceDetails.dbInstanceArn
resource.rds DbInstanceDetails.dbiResourceId
resource.rds DbInstanceDetails.dbSecurityGroups.name
resource.rds DbInstanceDetails.dbSecurityGroups.status
resource.rds DbInstanceDetails.engineVersion
resource.rds DbInstanceDetails.iamDatabaseAuthenticationEnabled
resource.rds DbInstanceDetails.publiclyAccessible
resource.rds DbInstanceDetails.vpcId
resource.rds DbInstanceDetails.vpcSecurityGroups.status
resource.rds DbInstanceDetails.vpcSecurityGroups.vpcSecurityGroupId
resource.rds DbUserDetails.application
resource.rds DbUserDetails.authMethod
resource.rds DbUserDetails.database
resource.rds DbUserDetails.ssl
resource.rds LimitlessDbDetails.dbClusterIdentifier
resource.rds LimitlessDbDetails.dbShardGroupArn
resource.rds LimitlessDbDetails.dbShardGroupIdentifier
resource.rds LimitlessDbDetails.dbShardGroupResourceId
resource.rds LimitlessDbDetails.engine
resource.rds LimitlessDbDetails.engineVersion

JSON-Feldname
resource.rds LimitlessDbDetails.tags.key
resource.rds LimitlessDbDetails.tags.value
resource.s3 BucketDetails.arn
ressource.s3 BucketDetails.createdAt
ressource.s3 BucketDetails.defaultServerSideEncryption.encryptionType
ressource.s3 BucketDetails.defaultServerSideEncryption.kmsMasterKeyArn
ressource.s3 BucketDetails.owner.id
ressource.s3 BucketDetails.publicAccess.permissionConfiguration.accountLevelPermissions.blockPublicAccess.blockPublicAcls
ressource.s3 BucketDetails.publicAccess.permissionConfiguration.accountLevelPermissions.blockPublicAccess.blockPublicPolicy
ressource.s3 BucketDetails.publicAccess.permissionConfiguration.accountLevelPermissions.blockPublicAccess.ignorePublicAcls
ressource.s3 BucketDetails.publicAccess.permissionConfiguration.accountLevelPermissions.blockPublicAccess.restrictPublicBuckets
ressource.s3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.accessControlList.allowsPublicReadAccess
ressource.s3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.accessControlList.allowsPublicWriteAccess
ressource.s3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.blockPublicAccess.blockPublicAcls
ressource.s3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.blockPublicAccess.blockPublicPolicy

JSON-Feldname
ressource.s3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.blockPublicAccess.ignorePublicAcls
ressource.s3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.blockPublicAccess.restrictPublicBuckets
ressource.s3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.bucketPolicy.allowsPublicReadAccess
ressource.s3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.bucketPolicy.allowsPublicWriteAccess
ressource.s3 BucketDetails.s3ObjectDetails.eTag
ressource.s3 BucketDetails.s3ObjectDetails.hash
ressource.s3 BucketDetails.s3ObjectDetails.key
ressource.s3 BucketDetails.s3ObjectDetails.objectArn
ressource.s3 BucketDetails.s3ObjectDetails.versionId
schemaVersion
service.action.aws ApiCallAction.domainDetails.domain
service.action.aws ApiCallAction.remoteIpDetails.country.countryCode
service.action.aws ApiCallAction.remoteIpDetails.geoLocation.lat
service.action.aws ApiCallAction.remoteIpDetails.geoLocation.lon
service.action.aws ApiCallAction.remoteIpDetails.organization.isp
service.action.aws ApiCallAction.remoteIpDetails.organization.org
service.action.aws ApiCallAction.userAgent
service.action.dns RequestAction.blocked

JSON-Feldname
service.action.dns RequestAction.protocol
service.action.kubernetes ApiCallAction.parameters
service.action.kubernetes ApiCallAction.remoteIpDetails.country.countryCode
service.action.kubernetes ApiCallAction.remoteIpDetails.geoLocation.lat
service.action.kubernetes ApiCallAction.remoteIpDetails.geoLocation.lon
service.action.kubernetes ApiCallAction.resource
service.action.kubernetes ApiCallAction.resourceName
service.action.kubernetes ApiCallAction.sourceIPs
service.action.kubernetes ApiCallAction.subresource
service.action.kubernetes ApiCallAction.userAgent
service.action.kubernetes ApiCallAction.verb
service.action.kubernetes PermissionCheckedDetails.allowed
service.action.kubernetes PermissionCheckedDetails.namespace
service.action.kubernetes PermissionCheckedDetails.resource
service.action.kubernetes PermissionCheckedDetails.verb
service.action.kubernetes RoleBindingDetails.kind
service.action.kubernetes RoleBindingDetails.name
service.action.kubernetes RoleBindingDetails.roleRefKind
service.action.kubernetes RoleBindingDetails.roleRefName
service.action.kubernetes RoleBindingDetails.uid

JSON-Feldname
service.action.kubernetes RoleDetails.kind
service.action.kubernetes RoleDetails.name
service.action.kubernetes RoleDetails.uid
service.action.netzwerk ConnectionAction.localNetworkInterface
service.action.netzwerk ConnectionAction.localPortDetails.portName
service.action.netzwerk ConnectionAction.remoteIpDetails.country.countryCode
service.action.netzwerk ConnectionAction.remoteIpDetails.geoLocation.lat
service.action.netzwerk ConnectionAction.remoteIpDetails.geoLocation.lon
service.action.netzwerk ConnectionAction.remoteIpDetails.organization.isp
service.action.netzwerk ConnectionAction.remoteIpDetails.organization.org
service.action.netzwerk ConnectionAction.remotePortDetails.portName
service.action.port ProbeAction.blocked
service.action.port ProbeAction.portProbeDetails.localIpDetails.ipAddressV4
service.action.port ProbeAction.portProbeDetails.localIpDetails.ipAddressV6
service.action.port ProbeAction.portProbeDetails.localPortDetails.port
service.action.port ProbeAction.portProbeDetails.localPortDetails.portName
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.city.cityName
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.country.countryCode
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.country.countryName
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.geoLocation.lat

JSON-Feldname
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.geoLocation.lon
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.ipAddressV4
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.ipAddressV6
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.organization.asn
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.organization.asnOrg
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.organization.isp
service.action.port ProbeAction.portProbeDetails.remoteIpDetails.organization.org
service.action.rds LoginAttemptAction.loginAttributes.application
service.action.rds LoginAttemptAction.loginAttributes.failedLoginAttempts
service.action.rds LoginAttemptAction.loginAttributes.successfulLoginAttempts
service.action.rds LoginAttemptAction.loginAttributes.user
service.action.rds LoginAttemptAction.remoteIpDetails.city.cityName
service.action.rds LoginAttemptAction.remoteIpDetails.country.countryCode
service.action.rds LoginAttemptAction.remoteIpDetails.country.countryName
service.action.rds LoginAttemptAction.remoteIpDetails.geoLocation.lat
service.action.rds LoginAttemptAction.remoteIpDetails.geoLocation.lon
service.action.rds LoginAttemptAction.remoteIpDetails.ipAddressV4
service.action.rds LoginAttemptAction.remoteIpDetails.ipAddressV6
service.action.rds LoginAttemptAction.remoteIpDetails.organization.asn
service.action.rds LoginAttemptAction.remoteIpDetails.organization.asnOrg

JSON-Feldname
service.action.rds LoginAttemptAction.remoteIpDetails.organization.isp
service.action.rds LoginAttemptAction.remoteIpDetails.organization.org
service.zusätzlich Info.agentDetails.agentId
Service.zusätzlich Info.agentDetails.agentVersion
Service.zusätzlich Info.anomalies.anomalousAPIs
Service.zusätzlich Info.authenticationMethod
Service.zusätzlich Info.averagePacketSizeIn
Service.zusätzlich Info.averagePacketSizeOut
Service.zusätzlich Info.context
Service.zusätzlich Info.domain
Service.zusätzlich Info.inBytes
Service.zusätzlich Info.localNetworkInterfaceOwner
Service.zusätzlich Info.localPort
Service.zusätzlich Info.outBytes
Service.zusätzlich Info.packetsIn
Service.zusätzlich Info.packetsOut
Service.zusätzlich Info.policyArn
Service.zusätzlich Info.policyName
Service.zusätzlich Info.remotePort
Service.zusätzlich Info.sample

JSON-Feldname
Service.zusätzlich Info.scannedPort
Service.zusätzlich Info.threatFileSha256
Service.zusätzlich Info.threatName
Service.zusätzlich Info.totalBytesIn
Service.zusätzlich Info.totalBytesOut
Service.zusätzlich Info.type
Service.zusätzlich Info.unusual.asnOrg
Service.zusätzlich Info.unusual.port
Service.zusätzlich Info.unusualProtocol
Service.zusätzlich Info.userAgent.fullUserAgent
Service.zusätzlich Info.userAgent.userAgentCategory
Service.zusätzlich Info.value
Service.zusätzlich Info.vpcOwnerAccountId
service.count
service.detection.sequence.actors.id
service.detection.sequence.actors.process.name
service.detection.sequence.actors.process.path
service.detection.sequence.actors.process.sha256
service.detection.sequence.actors.session.createdTime
service.detection.sequence.actors.session.issuer

JSON-Feldname
service.detection.sequence.actors.session.mfaStatus
service.detection.sequence.actors.session.uid
service.detection.sequence.actors.user.account.account
service.detection.sequence.actors.user.account.uid
service.detection.sequence.actors.user.CredentialUid
service.detection.sequence.actors.user.name
service.detection.sequence.actors.user.type
service.detection.sequence.actors.user.uid
service.detection.sequence.additional SequenceTypes
service.detection.sequence.description
service.detection.sequence.endpoints.autonomous System.name
service.detection.sequence.endpoints.autonomous System.number
service.detection.sequence.endpoints.connection.direction
service.detection.sequence.endpoints.domain
service.detection.sequence.endpoints.id
service.detection.sequence.endpoints.ip
service.detection.sequence.endpoints.location.city
service.detection.sequence.endpoints.location.country
service.detection.sequence.endpoints.location.lat
service.detection.sequence.endpoints.location.lon

JSON-Feldname
service.detection.sequence.endpoints.port
service.detection.sequence.resources.Account-ID
service.detection.sequence.resources.CloudPartition
service.detection.sequence.resources.data.access Key.principalId
service.detection.sequence.resources.data.access Key.userName
service.detection.sequence.resources.data.access Key.userType
service.detection.sequence.resources.data.autoscaling AutoScalingGroup.ec2InstanceUids
service.detection.sequence.resources.data.cloudformation Stack.ec2InstanceUids
service.detection.sequence.resources.data.container.image
service.detection.sequence.resources.data.container.imageUID
service.detection.sequence.resources.data.ec2 Image.ec2InstanceUids
service.detection.sequence.resources.data.ec2 Instance.availabilityZone
service.detection.sequence.resources.data.ec2 Instance.ec2NetworkInterfaceUids
service.detection.sequence.resources.data.ec2 Instance.iamInstanceProfile.arn
service.detection.sequence.resources.data.ec2 Instance.iamInstanceProfile.id
service.detection.sequence.resources.data.ec2 Instance.imageDescription
service.detection.sequence.resources.data.ec2 Instance.instanceState
service.detection.sequence.resources.data.ec2 Instance.instanceType
service.detection.sequence.resources.data.ec2 Instance.outpostArn
service.detection.sequence.resources.data.ec2 Instance.platform

JSON-Feldname
service.detection.sequence.resources.data.ec2 Instance.productCodes.productCodeId
service.detection.sequence.resources.data.ec2 Instance.productCodes.productCodeType
service.detection.sequence.resources.data.ec2 LaunchTemplate.ec2InstanceUids
service.detection.sequence.resources.data.ec2 LaunchTemplate.version
service.detection.sequence.resources.data.ec2 NetworkInterface.ipv6Addresses
service.detection.sequence.resources.data.ec2 NetworkInterface.privateIpAddresses.privateDnsName
service.detection.sequence.resources.data.ec2 NetworkInterface.privateIpAddresses.privateIpAddress
service.detection.sequence.resources.data.ec2 NetworkInterface.publicIp
service.detection.sequence.resources.data.ec2 NetworkInterface.securityGroups.groupId
service.detection.sequence.resources.data.ec2 NetworkInterface.securityGroups.groupName
service.detection.sequence.resources.data.ec2 NetworkInterface.subNetId
service.detection.sequence.resources.data.ec2 NetworkInterface.vpcId
service.detection.sequence.resources.data.ec2 Vpc.ec2InstanceUids
service.detection.sequence.resources.data.ecs Cluster.ec2InstanceUids
service.detection.sequence.resources.data.ecs Cluster.status
service.detection.sequence.resources.data.ecs Task.containerUids
service.detection.sequence.resources.data.ecs Task.createdAt
service.detection.sequence.resources.data.ecs Task.launchType
service.detection.sequence.resources.data.ecs Task.taskDefinitionArn

JSON-Feldname
service.detection.sequence.resources.data.eks Cluster.arn
service.detection.sequence.resources.data.eks Cluster.createdAt
service.detection.sequence.resources.data.eks Cluster.ec2InstanceUids
service.detection.sequence.resources.data.eks Cluster.status
service.detection.sequence.resources.data.eks Cluster.vpcId
service.detection.sequence.resources.data.iam InstanceProfile.ec2InstanceUids
service.detection.sequence.resources.data.iam InstanceProfile.id
service.detection.sequence.resources.data.kubernetes Workload.containerUids
service.detection.sequence.resources.data.kubernetes Workload.namespace
service.detection.sequence.resources.data.kubernetes Workload.type
service.detection.sequence.resources.data.s3 Bucket.accountPublicAccess.publicAclAccess
service.detection.sequence.resources.data.s3 Bucket.accountPublicAccess.publicAclIgnoreBehavior
service.detection.sequence.resources.data.s3 Bucket.accountPublicAccess.publicBucketRestrictBehavior
service.detection.sequence.resources.data.s3 Bucket.accountPublicAccess.publicPolicyAccess
service.detection.sequence.resources.data.s3 Bucket.bucketPublicAccess.publicAclAccess
service.detection.sequence.resources.data.s3 Bucket.bucketPublicAccess.publicAclIgnoreBehavior
service.detection.sequence.resources.data.s3 Bucket.bucketPublicAccess.publicBucketRestrictBehavior
service.detection.sequence.resources.data.s3 Bucket.bucketPublicAccess.publicPolicyAccess

JSON-Feldname
service.detection.sequence.resources.data.s3 Bucket.createdAt
service.detection.sequence.resources.data.s3 Bucket.effectivePermission
service.detection.sequence.resources.data.s3 Bucket.encryptionKeyArn
service.detection.sequence.resources.data.s3 Bucket.encryptionType
service.detection.sequence.resources.data.s3 Bucket.ownerId
service.detection.sequence.resources.data.s3 Bucket.publicReadAccess
service.detection.sequence.resources.data.s3 Bucket.publicWriteAccess
service.detection.sequence.resources.data.s3 Bucket.s3ObjectUids
service.detection.sequence.resources.data.s3 Object.eTag
service.detection.sequence.resources.data.s3 Object.key
service.detection.sequence.resources.data.s3 Object.versionId
service.detection.sequence.resources.name
service.detection.sequence.resources.region
service.detection.sequence.resources.ResourceType
service.detection.sequence.resources.service
service.detection.sequence.resources.tags.key
service.detection.sequence.resources.tags.value
service.detection.sequence.resources.uid
dienst.erkennung.sequenz.sequenz Indicators.key
dienst.erkennung.sequenz.sequenz Indicators.title

JSON-Feldname
dienst.erkennung.sequenz.sequenz Indicators.values
service.detection.sequence.signals.actorIds
service.detection.sequence.signals.count
service.detection.sequence.signals.CreatedAt
service.detection.sequence.signals.description
service.detection.sequence.signals.EndpointIds
service.detection.sequence.signals.first SeenAt
service.detection.sequence.signals.last SeenAt
dienst.erkennung.sequenz.signale.name
service.detection.sequence.signals.ResourceUIDs
service.detection.sequence.signals.severity
service.detection.sequence.signals.signal Indicators.key
dienste.erkennung.sequenz.signale.signal Indicators.title
dienste.erkennung.sequenz.signale.signal Indicators.values
service.detection.sequence.signale.type
service.detection.sequence.signals.uid
service.detection.sequence.signals.Aktualisiert am
service.detection.sequence.uid
service.detectorID
service.ebs VolumeScanDetails.scanCompletedAt

JSON-Feldname
service.ebs VolumeScanDetails.scanDetections.highestSeverityThreatDetails.count
service.ebs VolumeScanDetails.scanDetections.highestSeverityThreatDetails.severity
service.ebs VolumeScanDetails.scanDetections.highestSeverityThreatDetails.threatName
service.ebs VolumeScanDetails.scanDetections.scannedItemCount.files
service.ebs VolumeScanDetails.scanDetections.scannedItemCount.totalGb
service.ebs VolumeScanDetails.scanDetections.scannedItemCount.volumes
service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.itemCount
service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.shortened
service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.filePaths.fileName
service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.filePaths.filePath
service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.filePaths.volumeArn
service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.itemCount
service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.uniqueThreatNameCount
service.ebs VolumeScanDetails.scanDetections.threatsDetectedItemCount.files
service.ebs VolumeScanDetails.scanStartedAt
service.ebs VolumeScanDetails.scanType
service.ebs VolumeScanDetails.sources
service.veranstaltung FirstSeen
Service.Veranstaltung LastSeen

JSON-Feldname
Service.Malware ScanDetails.scanCategory
Service.Malware ScanDetails.scanConfiguration.incrementalScanDetails.baselineResourceArn
Service.Malware ScanDetails.scanConfiguration.triggerType
Service.Malware ScanDetails.threats.count
Service.Malware ScanDetails.threats.hash
Service.Malware ScanDetails.threats.itemDetails.additionalInfo.deviceName
Service.Malware ScanDetails.threats.itemDetails.additionalInfo.versionId
Service.Malware ScanDetails.threats.itemDetails.hash
Service.Malware ScanDetails.threats.itemDetails.itemPath
Service.Malware ScanDetails.threats.itemDetails.resourceArn
Service.Malware ScanDetails.threats.itemPaths.hash
Service.Malware ScanDetails.threats.itemPaths.nestedItemPath
Service.Malware ScanDetails.threats.source
Service.Malware ScanDetails.uniqueThreatCount
service.runtime Details.context.addressFamily
service.runtime Details.context.commandLineExample
service.runtime Details.context.fileSystemType
service.runtime Details.context.flags
service.runtime Details.context.ianaProtocolNumber
service.runtime Details.context.ldPreloadValue

JSON-Feldname
service.runtime Details.context.libraryPath
service.runtime Details.context.memoryRegions
service.runtime Details.context.modifiedAt
service.runtime Details.context.modifyingProcess.euid
service.runtime Details.context.modifyingProcess.executablePath
service.runtime Details.context.modifyingProcess.executableSha256
service.runtime Details.context.modifyingProcess.lineage.euid
service.runtime Details.context.modifyingProcess.lineage.executablePath
service.runtime Details.context.modifyingProcess.lineage.name
service.runtime Details.context.modifyingProcess.lineage.namespacePid
service.runtime Details.context.modifyingProcess.lineage.parentUuid
service.runtime Details.context.modifyingProcess.lineage.pid
service.runtime Details.context.modifyingProcess.lineage.startTime
service.runtime Details.context.modifyingProcess.lineage.userId
service.runtime Details.context.modifyingProcess.lineage.uuid
service.runtime Details.context.modifyingProcess.name
service.runtime Details.context.modifyingProcess.namespacePid
service.runtime Details.context.modifyingProcess.parentUuid
service.runtime Details.context.modifyingProcess.pid
service.runtime Details.context.modifyingProcess.pwd

JSON-Feldname
service.runtime Details.context.modifyingProcess.startTime
service.runtime Details.context.modifyingProcess.user
service.runtime Details.context.modifyingProcess.userId
service.runtime Details.context.modifyingProcess.uuid
service.runtime Details.context.mountSource
service.runtime Details.context.mountTarget
service.runtime Details.context.relatedFilePaths
service.runtime Details.context.releaseAgentPath
service.runtime Details.context.runcBinaryPath
service.runtime Details.context.scriptPath
service.runtime Details.context.serviceName
service.runtime Details.context.shellHistoryFilePath
service.runtime Details.context.socketPath
service.runtime Details.context.targetProcess.euid
service.runtime Details.context.targetProcess.executablePath
service.runtime Details.context.targetProcess.executableSha256
service.runtime Details.context.targetProcess.lineage.euid
service.runtime Details.context.targetProcess.lineage.executablePath
service.runtime Details.context.targetProcess.lineage.name
service.runtime Details.context.targetProcess.lineage.namespacePid

JSON-Feldname
service.runtime Details.context.targetProcess.lineage.parentUuid
service.runtime Details.context.targetProcess.lineage.pid
service.runtime Details.context.targetProcess.lineage.startTime
service.runtime Details.context.targetProcess.lineage.userId
service.runtime Details.context.targetProcess.lineage.uuid
service.runtime Details.context.targetProcess.name
service.runtime Details.context.targetProcess.namespacePid
service.runtime Details.context.targetProcess.parentUuid
service.runtime Details.context.targetProcess.pid
service.runtime Details.context.targetProcess.pwd
service.runtime Details.context.targetProcess.startTime
service.runtime Details.context.targetProcess.user
service.runtime Details.context.targetProcess.userId
service.runtime Details.context.targetProcess.uuid
service.runtime Details.context.threatFilePath
service.runtime Details.context.toolCategory
service.runtime Details.context.toolName
service.runtime Details.process.euid
service.runtime Details.process.lineage.euid
service.runtime Details.process.lineage.executablePath

JSON-Feldname
service.runtime Details.process.lineage.name
service.runtime Details.process.lineage.namespacePid
service.runtime Details.process.lineage.parentUuid
service.runtime Details.process.lineage.pid
service.runtime Details.process.lineage.startTime
service.runtime Details.process.lineage.userId
service.runtime Details.process.lineage.uuid
service.runtime Details.process.namespacePid
service.runtime Details.process.parentUuid
service.runtime Details.process.pid
service.runtime Details.process.pwd
service.runtime Details.process.startTime
service.runtime Details.process.user
service.runtime Details.process.userId
service.runtime Details.process.uuid
service.Benutzerfeedback

Unterdrückungsregeln in GuardDuty

Eine Unterdrückungsregel ist eine Reihe von Kriterien, die zum Filtern von Erkenntnissen verwendet werden, indem neue Erkenntnisse, die den angegebenen Kriterien entsprechen, automatisch archiviert werden. Unterdrückungsregeln können verwendet werden, um Ergebnisse mit niedrigem Wert, falsch positive Ergebnisse oder Bedrohungen zu filtern, auf die Sie nicht reagieren möchten,

sodass die Sicherheitsbedrohungen mit den meisten Auswirkungen auf Ihre Umgebung leichter zu erkennen sind.

Nachdem Sie eine Unterdrückungsregel erstellt haben, werden neue Ergebnisse, die den in der Regel definierten Kriterien entsprechen, automatisch archiviert, solange die Unterdrückungsregel gültig ist. Sie können einen vorhandenen Filter verwenden, um eine Unterdrückungsregel zu erstellen, oder einen neuen Filter für die Unterdrückungsregel definieren, während Sie sie erstellen. Sie können Unterdrückungsregeln so konfigurieren, dass ganze Ergebnistypen unterdrückt werden, oder detailliertere Filterkriterien definieren, damit nur bestimmte Instances eines bestimmten Ergebnistyps unterdrückt werden. Sie können die Unterdrückungsregeln jederzeit bearbeiten.

Unterdrückte Ergebnisse werden nicht an Amazon Simple Storage Service AWS Security Hub CSPM, Amazon Detective oder Amazon gesendet. Dadurch wird das Störgeräusch reduziert EventBridge, wenn Sie die GuardDuty Ergebnisse über Security Hub CSPM, ein SIEM eines Drittanbieters oder andere Warn- und Ticketing-Anwendungen nutzen. Wenn Sie diese Option aktiviert habenMalware-Schutz für EC2, wird aufgrund der unterdrückten GuardDuty Ergebnisse kein Malware-Scan ausgelöst.

GuardDuty generiert weiterhin Ergebnisse, auch wenn sie Ihren Unterdrückungsregeln entsprechen. Diese Ergebnisse werden jedoch automatisch als archiviert markiert. Das archivierte Ergebnis wird 90 Tage lang gespeichert und kann in GuardDuty diesem Zeitraum jederzeit eingesehen werden. Sie können die unterdrückten Ergebnisse in der GuardDuty Konsole anzeigen, indem Sie in der Ergebnistabelle die Option Archiviert auswählen, oder verwenden Sie die ListFindings API mit dem `findingCriteria` Kriterium „Wahr`service.archived`“. GuardDuty

> **Note**
>
> In einer Umgebung mit mehreren Konten kann nur der GuardDuty Administrator Unterdrückungsregeln erstellen.

Verwendung von Unterdrückungsregeln mit Extended Threat Detection

GuardDuty Extended Threat Detection erkennt automatisch mehrstufige Angriffe, die sich über Datenquellen, mehrere Arten von AWS Ressourcen und Zeiträume erstrecken, innerhalb eines AWS-Konto. Es korreliert Ereignisse aus verschiedenen Datenquellen, um Szenarien zu identifizieren, die sich als potenzielle Bedrohung für Ihre AWS Umgebung darstellen, und generiert dann eine Analyse der Angriffssequenz. Weitere Informationen finden Sie unter So funktioniert Extended Threat Detection.

Wenn Sie Unterdrückungsregeln erstellen, mit denen Ergebnisse archiviert werden, kann Extended Threat Detection diese archivierten Ergebnisse nicht verwenden, um Ereignisse für Angriffssequenzen zu korrelieren. Umfassende Unterdrückungsregeln können die Fähigkeit beeinträchtigen, Verhaltensweisen GuardDuty zu erkennen, die mit der Erkennung mehrstufiger Angriffe einhergehen. Ergebnisse, die aufgrund von Unterdrückungsregeln archiviert werden, gelten nicht als Signale für Angriffssequenzen. Wenn Sie beispielsweise eine Unterdrückungsregel erstellen, die alle EKS-Cluster-bezogenen Ergebnisse archiviert, anstatt auf bestimmte bekannte Aktivitäten abzuzielen, können Sie diese Ergebnisse GuardDuty nicht verwenden, um eine Angriffssequenz zu erkennen, bei der ein Bedrohungsakteur einen Container ausnutzt, privilegierte Token erhält und auf vertrauliche Ressourcen zugreift.

Beachten Sie die folgenden Empfehlungen von: GuardDuty

- Verwenden Sie weiterhin Unterdrückungsregeln, um Warnmeldungen aufgrund bekannter vertrauenswürdiger Aktivitäten zu reduzieren.
- Konzentrieren Sie sich bei den Unterdrückungsregeln auf bestimmte Verhaltensweisen, für die Sie keine Ergebnisse generieren GuardDuty möchten.

Häufige Anwendungsfälle für Unterdrückungsregeln und Beispiele

Die folgenden Ergebnisarten haben häufig Anwendungsfälle für die Anwendung von Unterdrückungsregeln. Wählen Sie den Namen des Ergebnisses aus, um mehr über das Ergebnis zu erfahren. Lesen Sie die Beschreibung des Anwendungsfalls, um zu entscheiden, ob Sie eine Unterdrückungsregel für diesen Befundtyp erstellen möchten.

> **Important**
>
> GuardDuty empfiehlt, Unterdrückungsregeln reaktiv und nur für Ergebnisse zu erstellen, für die Sie in Ihrer Umgebung wiederholt Fehlalarme identifiziert haben.

- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS – Verwenden Sie eine Unterdrückungsregel, die automatisch Erkenntnisse archiviert, die generiert werden, falls das VPC-Netzwerk so konfiguriert ist, dass der Internet-Datenverkehr über ein On-Premises-Gateway anstelle eines VPC-Internet-Gateways weitergeleitet wird.

  Diese Erkenntnis wird generiert, wenn das Netzwerk so konfiguriert ist, dass der Internetverkehr von einem On-Premises-Gateway und nicht von einem VPC Internet Gateway (IGW) ausgeht.

Geläufige Konfigurationen, z. B. die Verwendung von AWS Outposts, oder VPC-VPN-Verbindungen, können dazu führen, dass Datenverkehr auf diese Weise weitergeleitet wird. Wenn dieses Verhalten erwartet wird, wird empfohlen, Unterdrückungsregeln zu verwenden und eine Regel zu erstellen, die aus zwei Filterkriterien besteht. Das erste Kriterium ist der Erkenntnistyp, der `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS` sein sollte. Das zweite Filterkriterium ist die IPv4-Adresse des API-Aufrufers mit der IP-Adresse oder dem CIDR-Bereich Ihres On-Premises-Internet-Gateways. Das folgende Beispiel stellt den Filter dar, den Sie verwenden würden, um diesen Erkenntnistyp auf der Grundlage der IP-Adresse des API-Aufrufers zu unterdrücken.

```
Finding type: UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
 API caller IPv4 address: 198.51.100.6
```

> **Note**
>
> Um mehrere API-Aufrufer-IPs einzubeziehen, können Sie jede IP-Adresse zur Werteliste für Gleich oder NotEquals Bedingungen hinzufügen oder Platzhaltermuster für Übereinstimmungen oder Bedingungen verwenden. NotMatches

- Recon:EC2/Portscan – Verwenden Sie eine Unterdrückungsregel, um Erkenntnisse automatisch zu aktivieren, wenn Sie eine Anwendung für Schwachstellenanalysen verwenden.

  Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Erkenntnistyp mit dem Wert `Recon:EC2/Portscan` verwenden. Das zweite Filterkriterium sollte den Instances entsprechen, die diese Tools zur Schwachstellenanalyse hosten. Sie können entweder das Attribut Instance-Image-ID oder das Attribut Tag verwenden, abhängig davon, welches Kriterium mit den Instances identifiziert werden kann, die diese Tools hosten. Das folgende Beispiel stellt den Filter dar, den Sie verwenden würden, um diesen Erkenntnistyp auf der Grundlage von Instances mit einem bestimmten AMI zu unterdrücken.

  ```
  Finding type: Recon:EC2/Portscan Instance image ID: ami-999999999
  ```

- UnauthorizedAccess:EC2/SSHBruteForce – Verwenden Sie eine Unterdrückungsregel, um Erkenntnisse, die sich auf Bastion-Instances beziehen, automatisch zu archivieren.

  Wenn das Ziel des Brute-Force-Versuchs ein Bastion-Host ist, kann dies das erwartete Verhalten in Ihrer Umgebung darstellen. AWS In diesem Fall sollten Sie für diese Erkenntnis eine Unterdrückungsregel einrichten. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen.

Das erste Kriterium sollte das Attribut Erkenntnistyp mit dem Wert `UnauthorizedAccess:EC2/SSHBruteForce` verwenden. Das zweite Filterkriterium sollte der oder den Instances entsprechen, die als Bastion-Host eingesetzt werden. Sie können entweder das Attribut Instance-Image-ID oder das Attribut Tag verwenden, abhängig davon, welches Kriterium mit den Instances identifiziert werden kann, die diese Tools hosten. Das folgende Beispiel stellt den Filter dar, den Sie verwenden würden, um diesen Erkenntnistyp auf der Grundlage von Instances mit einem bestimmten Instance-Tag-Wert zu unterdrücken.

```
Finding type: UnauthorizedAccess:EC2/SSHBruteForce Instance tag value: devops
```

- Recon:EC2/PortProbeUnprotectedPort – Verwenden Sie eine Unterdrückungsregel, um Erkenntnisse automatisch zu archivieren, wenn sie auf absichtlich exponierte Instances ausgerichtet ist.

  In einigen Fällen werden Instances absichtlich exponiert, weil sie beispielsweise Webserver hosten. Wenn dies in Ihrer AWS Umgebung der Fall ist, empfehlen wir Ihnen, eine Unterdrückungsregel für diesen Befund einzurichten. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Erkenntnistyp mit dem Wert `Recon:EC2/PortProbeUnprotectedPort` verwenden. Das zweite Filterkriterium sollte der oder den Instances entsprechen, die als Bastion-Host eingesetzt werden. Sie können entweder das Attribut Instance-Image-ID oder das Attribut Tag verwenden, abhängig davon, welches Kriterium mit den Instances identifiziert werden kann, die diese Tools hosten. Das folgende Beispiel stellt den Filter dar, den Sie verwenden würden, um diesen Erkenntnistyp auf der Grundlage von Instances mit einem bestimmten Instance-Tag-Schlüssel in der Konsole zu unterdrücken.

  ```
  Finding type: Recon:EC2/PortProbeUnprotectedPort Instance tag key: prod
  ```

Empfohlene Unterdrückungsregeln für Ergebnisse der Laufzeitüberwachung

- PrivilegeEscalation:Runtime/DockerSocketAccessed wird generiert, wenn ein Prozess in einem Container mit dem Docker-Socket kommuniziert. Möglicherweise gibt es Container in Ihrer Umgebung, die aus legitimen Gründen auf den Docker-Socket zugreifen müssen. Der Zugriff von solchen Containern generiert PrivilegeEscalation:Runtime/DockerSocketAccessed-Erkenntnisse. Wenn dies in Ihrer AWS Umgebung der Fall ist, empfehlen wir Ihnen, eine Unterdrückungsregel für diesen Ergebnistyp einzurichten. Das erste Kriterium sollte das Attribut Erkenntnistyp mit dem Wert `PrivilegeEscalation:Runtime/DockerSocketAccessed` verwenden. Das zweite Filterkriterium ist das Feld Ausführbarer Pfad mit einem Wert, der dem Wert des

Prozesses `executablePath` in der generierten Erkenntnis entspricht. Alternativ kann das zweite Filterkriterium das SHA-256 Feld Ausführbar verwenden, dessen Wert dem Wert des Prozesses `executableSha256` im generierten Ergebnis entspricht.

- Kubernetes-Cluster führen ihre eigenen DNS-Server als Pods aus, z. B. `coredns`. Daher werden bei jeder DNS-Suche aus einem Pod zwei DNS-Ereignisse GuardDuty erfasst — eines aus dem Pod und das andere aus dem Server-Pod. Dadurch können Duplikate für die folgenden DNS-Erkenntnisse generiert werden:
  - Backdoor:Runtime/C&CActivity.B! DNS
  - CryptoCurrency:Runtime/BitcoinTool.B! DNS
  - Impact:Runtime/AbusedDomainRequest.Reputation
  - Impact:Runtime/BitcoinDomainRequest.Reputation
  - Impact:Runtime/MaliciousDomainRequest.Reputation
  - Impact:Runtime/SuspiciousDomainRequest.Reputation
  - Trojan:Runtime/BlackholeTraffic! DNS
  - Trojan:Runtime/DGADomainRequest.C! DNS
  - Trojan:Runtime/DriveBySourceTraffic! DNS
  - Trojan:Runtime/DropPoint! DNS
  - Trojan:Runtime/PhishingDomainRequest! DNS

  Die doppelten Erkenntnisse umfassen Pod-, Container- und Prozessdetails, die Ihrem DNS-Server-Pod entsprechen. Sie können mithilfe dieser Felder eine Unterdrückungsregel einrichten, um diese doppelten Erkenntnisse zu unterdrücken. Die ersten Filterkriterien sollten das Feld Erkenntnistyp verwenden, dessen Wert einem DNS-Erkenntnistyp aus der Liste der Erkenntnisse entspricht, die weiter oben in diesem Abschnitt bereitgestellt wurde. Das zweite Filterkriterium könnte entweder der Pfad der ausführbaren Datei mit dem Wert Ihres DNS-Servers `executablePath` oder die Ausführbare Datei SHA-256 mit einem Wert sein, der dem Wert Ihres DNS-Servers `executableSHA256` im generierten Ergebnis entspricht. Als optionales drittes Filterkriterium können Sie das Feld Kubernetes-Container-Image verwenden, dessen Wert dem Container-Image Ihres DNS-Server-Pods in der generierten Erkenntnis entspricht.

Unterdrückungsregeln erstellen in GuardDuty

Eine Unterdrückungsregel besteht aus einer Reihe von Kriterien, die die Verwendung von Filterattributen und die Angabe von Werten umfassen, für die Sie keinen Ergebnistyp generieren

GuardDuty möchten. Die Ergebnisarten, die diesen Kriterien entsprechen, werden automatisch archiviert. Um das Rauschen zu reduzieren, werden die unterdrückten Ergebnisse an keine der Organisationen gesendet, in die Sie möglicherweise integrieren. AWS-Services Weitere Informationen zu häufigen Anwendungsfällen beim Erstellen von Unterdrückungsregeln finden Sie unterUnterdrückungsregeln.

Mithilfe der Seite „Unterdrückungsregeln“ in der GuardDuty Konsole können Sie Unterdrückungsregeln visualisieren, erstellen und verwalten. Unterdrückungsregeln können auch aus Ihren vorhandenen gespeicherten Filtern generiert werden. Weitere Informationen zum Erstellen von Filtern finden Sie unter Ergebnisse filtern in GuardDuty.

Die Filterkriterien können eine exakte Übereinstimmung mit Gleichheitszeichen und NotEquals Operatoren, eine Platzhalterübereinstimmung mit den Operatoren Treffer und NotMatches Operatoren oder Vergleichsübereinstimmung mit GreaterThan LessThan und LessThanEquals umfassen. GreaterThanEquals Weitere Informationen zu den verfügbaren Operatoren finden Sie auf der Conditions Seite.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um eine Unterdrückungsregel für die GuardDuty Suche nach Typen zu erstellen.

Console

So erstellen Sie eine Unterdrückungsregel mithilfe der Konsole:

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Klicken Sie auf der Seite Unterdrückungsregeln auf Unterdrückungsregel erstellen, um das Formular Unterdrückungsregel erstellen zu öffnen.
3. Geben Sie einen Namen für die Unterdrückungsregel ein. Der Name muss 3 bis 64 Zeichen lang sein. Gültige Zeichen sind a-z A-Z, 0-9, Punkt (.), Bindestrich (-) und Unterstrich (_).
4. Die Beschreibung ist optional. Wenn Sie eine Beschreibung eingeben, kann diese bis zu 512 Zeichen lang sein. Gültige Zeichen sind a-z A-Z, 0-9, Punkt (.), Bindestrich (-), Doppelpunkt (:), Klammern ({} () []), Schrägstrich (/) und Leerzeichen.
5. Der Rang ist optional. Es kann ein numerischer Wert von 1 bis zur Gesamtzahl der Filter und Unterdrückungsregeln plus 1 sein.
6. Wählen Sie im Abschnitt Attribute einen Schlüssel und einen Operator aus der Dropdownliste aus.
7. Geben Sie den Wert entweder „Zeichenfolge“ oder „Datum“ aus dem Datepicker ein, basierend auf dem ausgewählten Schlüssel. Wenn es sich um einen Zeichenkettenwert

handelt, geben Sie den Text ein und drücken Sie die Eingabetaste. Bei Zeichenkettenwerten können mehrere Werte hinzugefügt werden.

8. Zusätzliche Kriterien können hinzugefügt werden, indem Sie Kriterien hinzufügen auswählen, um einen weiteren Satz von Schlüsseln, Operatoren und Werten hinzuzufügen.
9. Wählen Sie Unterdrückungsregel erstellen aus, um die Unterdrückungsregel zu erstellen und zu speichern.

Sie können auch eine Unterdrückungsregel aus einem vorhandenen gespeicherten Filter erstellen. Weitere Informationen zum Erstellen von Filtern finden Sie unter Ergebnisse filtern in GuardDuty.

So erstellen Sie eine Unterdrückungsregel aus einem gespeicherten Filter:

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie auf der Seite Ergebnisse im Menü Gespeicherte Regeln eine gespeicherte Filtersatzregel aus. Dadurch werden automatisch der Filtersatz und die Ergebnisse angezeigt, die den Kriterien entsprechen.
3. Sie können dieser gespeicherten Regel auch weitere Filterkriterien hinzufügen. Wenn Sie keine zusätzlichen Filterkriterien benötigen, überspringen Sie diesen Schritt. Um ein oder mehrere Filterkriterien hinzuzufügen, folgen Sie den Schritten 3 bis 7 und fahren Sie dann mit den folgenden Schritten fort. Adding filters on Findings page
4. Nachdem Sie die Filterkriterien hinzugefügt und bestätigt haben, dass die gefilterten Ergebnisse Ihren Anforderungen entsprechen, wählen Sie Unterdrückungsregel erstellen aus.
5. Geben Sie einen Namen für die Unterdrückungsregel ein. Der Name muss 3 bis 64 Zeichen lang sein. Gültige Zeichen sind a-z, 0-9 A-Z, Punkt (.), Bindestrich (-) und Unterstrich (_).
6. Die Beschreibung ist optional. Wenn Sie eine Beschreibung eingeben, kann diese bis zu 512 Zeichen lang sein.
7. Wählen Sie Erstellen aus.
8. Wenn Sie der gespeicherten Regel keine zusätzlichen Filterkriterien hinzufügen müssen, führen Sie die Schritte 4 bis 7 aus, um den Filter zu erstellen.

API/CLI

So erstellen Sie eine Unterdrückungsregel mithilfe der API:

1. Sie können Unterdrückungsregeln auch über die CreateFilter-API erstellen. Geben Sie dazu die Filterkriterien in einer JSON-Datei an und folgen Sie dabei dem Format des unten beschriebenen Beispiels. Im folgenden Beispiel werden alle unarchivierten Ergebnisse mit niedrigem Schweregrad unterdrückt, für die eine DNS-Anfrage an die `test.example.com` Domain gestellt wurde. Bei Befunden mit mittlerem Schweregrad wird die Eingabeliste wie folgt angezeigt. `["4", "5", "7"]` Bei Befunden mit hohem Schweregrad lautet die Eingabeliste wie folgt`["6", "7", "8"]`. Bei Befunden mit kritischem Schweregrad lautet die Eingabeliste wie folgt`["9", "10"]`. Sie können auch auf der Grundlage eines beliebigen Werts in der Liste filtern.

   Im folgenden Beispiel wird ein Filter für Ergebnisse mit niedrigem Schweregrad für Lambda-Funktionen mit dem Funktionsnamenpräfix "MyFunc" und dem Funktions-Tag mit dem Präfix nicht als "“ TestTag hinzugefügt

   ```
   {
       "Criterion": {
           "service.action.dnsRequestAction.domain": {
               "Equals": [
                   "test.example.com"
               ]
           },
           "severity": {
               "Equals": [
                   "1",
                   "2",
                   "3"
               ]
           }
       }
   }
   ```

   Sie können Unterdrückungsregeln mithilfe der Platzhalterzeichen * und? erstellen . Platzhalter in Filtern werden nur bei Verwendung von Matches und NotMatches Operatoren unterstützt. Um eine beliebige Anzahl von Zeichen abzugleichen, können Sie * im Attributwert

verwenden. Um ein einzelnes Zeichen abzugleichen, können Sie? im Attributwert. Filter unterstützen maximal 5 Attribute unter einer einzigen Platzhalterbedingung und maximal 5 Platzhalterzeichen innerhalb eines einzelnen Attributs. Das folgende Beispiel fügt einen Filter für den Lambda-Namen hinzu, der dem Präfix „MyFunc" entspricht, aber keine Lambda-Funktionen mit Tags mit "TestTag" als Präfix, gefolgt von 0-2 Zeichen.

```
{
    "Criterion": {
        "resource.lambdaDetails.functionName": {
            "Matches": [
                "MyFunc*"
            ]
        },
        "resource.lambdaDetails.tags.key": {
            "NotMatches": [
                "TestTag??"
            ]
        }
    }
}
```

Eine Liste der JSON-Feldnamen und deren Konsolenäquivalent finden Sie unter Eigenschaftsfilter in GuardDuty.

Verwenden Sie zum Testen Ihrer Filterkriterien dasselbe JSON-Kriterium in der ListFindings-API und vergewissern Sie sich, dass die richtigen Erkenntnisse ausgewählt wurden. AWS CLI Folgen Sie dem Beispiel, um Ihre Filterkriterien anhand Ihrer eigenen DetectorID- und JSON-Datei zu testen.

Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die API aus. `detectorId` ListDetectors

```
aws guardduty list-detector
```

```
aws guardduty list-findings \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
```

```
--region us-east-1 \
--finding-criteria file://criteria.json
```

> **Note**
>
> Passende Platzhalter sind für ListFindings und GetFindingsStatistics nicht verfügbar. Kriterien, die Platzhalter enthalten, können nicht mit ListFindings und validiert werden. GetFindingsStatistics

2. Laden Sie Ihren Filter, der als Unterdrückungsregel verwendet werden soll, mit der CreateFilter-API oder über die AWS -CLI hoch, indem Sie dem unten stehenden Beispiel folgen und Ihre eigene Detektor-ID, einen Namen für die Unterdrückungsregel und eine JSON-Datei angeben.

   Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

```
aws guardduty create-filter \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--region us-east-1 \
--action ARCHIVE \
--name yourfiltername \
--finding-criteria file://criteria.json
```

Mit der ListFilter-API können Sie sich programmgesteuert eine Liste Ihrer Filter anzeigen lassen. Sie können die Details eines einzelnen Filters anzeigen, indem Sie der GetFilter-API den Filternamen zur Verfügung stellen. Aktualisieren Sie Filter mithilfe von UpdateFilter oder löschen Sie sie mit der DeleteFilter-API.

Aktualisierung der Unterdrückungsregeln in GuardDuty

In diesem Abschnitt werden die Schritte zum Aktualisieren einer Unterdrückungsregel AWS-Konto in Ihrem eigenen Ordner beschrieben AWS-Region.

Sie können bestehende Unterdrückungsregeln auf der Seite „Unterdrückungsregeln“ in der GuardDuty Konsole aktualisieren. GuardDuty unterstützt das Aktualisieren der Beschreibung, des Rangs und der Filterkriterien für den Unterdrückungsfilter über die GuardDuty Konsole oder mithilfe der GuardDuty CLI/API. Beim Aktualisieren der Unterdrückungsregel gelten dieselben Einschränkungen in Bezug auf die Feldwerte für Beschreibung, Rang und Kriterien wieUnterdrückungsregeln erstellen.

Wenn Sie ein Mitgliedskonto sind, kann Ihr Administratorkonto diese Aktion in Ihrem Namen ausführen. Weitere Informationen finden Sie unter Beziehungen zwischen Administratorkonto und Mitgliedskonto.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um eine Unterdrückungsregel für GuardDuty Findingtypes zu löschen.

Console

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/
2. Wählen Sie auf der Seite Unterdrückungsregeln die Unterdrückungsregel aus, die aktualisiert werden soll.
3. Wählen Sie in der Dropdownliste Aktionen die Option Unterdrückungsregel aktualisieren aus.
4. Dadurch wird das bestehende Formular für die Unterdrückungsregel geöffnet.
5. Nehmen Sie nach Bedarf Änderungen an den Abschnitten Beschreibung, Rang und Attribute vor.
6. Wählen Sie Unterdrückungsregel aktualisieren aus, um die Unterdrückungsregel zu aktualisieren.

API/CLI

Um eine Unterdrückungsregel mithilfe der API zu aktualisieren:

1. Sie können die Unterdrückungsregeln über die UpdateFilter API aktualisieren. Nur Beschreibung, Rang und Kriterien können mithilfe der UpdateFilter API aktualisiert werden. Alle diese drei Felder sind optional.
2. Um einen vorhandenen Filter zu aktualisieren, benötigen Sie den Namen des Filters, den Sie aktualisieren möchten.

3. Wenn Sie die vorhandenen Kriterien aktualisieren möchten, erstellen Sie eine JSON-Datei mit den aktualisierten Kriterien, ähnlich wie Sie den Filter zuerst erstellt haben. Ein Beispielkriterium zur Unterdrückung unarchivierter Ergebnisse mit niedrigem Schweregrad, die eine DNS-Anfrage an die Domain test.example.com enthalten. Bei Befunden mit mittlerem Schweregrad lautet die Eingabeliste ["4", „5", „7"]. Bei Befunden mit hohem Schweregrad lautet die Eingabeliste ["6", „7", „8"]. Bei Befunden mit kritischem Schweregrad lautet die Eingabeliste ["9", „10"]. Sie können auch auf der Grundlage eines beliebigen Werts in der Liste filtern. Im folgenden Beispiel wird ein Filter für Ergebnisse mit niedrigem Schweregrad hinzugefügt.

```
{
    "Criterion": {
        "service.action.dnsRequestAction.domain": {
            "Equals": [
                "test.example.com"
            ]
        },
        "severity": {
            "Equals": [
                "1",
                "2",
                "3"
            ]
        }
    }
}
```

Eine Liste der JSON-Feldnamen und deren Konsolenäquivalent finden Sie unter Eigenschaftsfilter in GuardDuty.

Verwenden Sie zum Testen Ihrer Filterkriterien dasselbe JSON-Kriterium in der ListFindings-API und vergewissern Sie sich, dass die richtigen Erkenntnisse ausgewählt wurden. AWS CLI Folgen Sie dem Beispiel, um Ihre Filterkriterien anhand Ihrer eigenen DetectorID- und JSON-Datei zu testen.

Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen" in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die API aus. `detectorId` ListDetectors

```
aws guardduty list-detectors --region us-east-1
```

4. Wenn Sie die Beschreibung aktualisieren möchten, können Sie den Beschreibungsparameter in den CLI-Aufruf aufnehmen.
5. Wenn Sie den Rang aktualisieren möchten, können Sie den Rank-Parameter in den CLI-Aufruf aufnehmen.
6. Wenn Sie von einem Unterdrückungsfilter auf einen regulären Filter aktualisieren möchten, verwenden Sie den Aktionsparameter und den Wert als ARCHIVE im CLI-Aufruf.
7. Aktualisieren Sie Ihre bestehende Filter-API oder verwenden Sie das AWS CLI folgende Beispiel mit Ihrer eigenen Detektor-ID, einem Namen für die Unterdrückungsregel und einer.json-Datei.
8. Im Folgenden finden Sie ein Beispiel für eine CLI, die alle oben beschriebenen Parameter aktualisiert. Sie können die spezifischen Parameter, die für Ihren Anwendungsfall aktualisiert werden sollen, mit dem Befehl - auswählen

```
aws guardduty update-filter \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--region us-east-1 \
--action ARCHIVE \
--rank 1 \
--description "Updated description" \
--finding-criteria file://criteria.json
```

Löschen von Unterdrückungsregeln in GuardDuty

In diesem Abschnitt werden die Schritte zum Löschen einer Unterdrückungsregel AWS-Konto in Ihrem Ordner beschrieben AWS-Region.

Möglicherweise möchten Sie eine Unterdrückungsregel löschen, die in Ihrer Umgebung kein erwartetes Verhalten mehr zeigt. Sie möchten den zugehörigen Ergebnistyp nicht mehr unterdrücken, sodass ein Ergebnistyp generiert GuardDuty werden kann.

Wenn Sie ein Mitgliedskonto sind, kann Ihr Administratorkonto diese Aktion in Ihrem Namen ausführen. Weitere Informationen finden Sie unter Beziehungen zwischen Administratorkonto und Mitgliedskonto.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um eine Unterdrückungsregel für die GuardDuty Suche nach Typen zu löschen.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie auf der Seite Unterdrückungsregeln die Unterdrückungsregel aus, die gelöscht werden soll.
3. Wählen Sie in der Dropdownliste Aktionen die Option Unterdrückungsregel löschen aus.
4. Es öffnet sich ein Bestätigungs-Popup. Wählen Sie Löschen, um mit dem Löschen fortzufahren. Oder wählen Sie Abbrechen, um den Vorgang abzubrechen.

API/CLI

Führen Sie die API DeleteFilter aus. Geben Sie den Filternamen und die zugehörige Detektor-ID für die jeweilige Region an.

Alternativ können Sie das folgende AWS CLI Beispiel verwenden, indem Sie die in *red* formatierten Werte ersetzen:

```
aws guardduty delete-filter \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--filter-name filterName \
--region us-east-1
```

Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

Metriken zur Unterdrückung von Regeln

Mit Amazon können Sie überwachen GuardDuty, wie oft die einzelnen Unterdrückungsregeln übereinstimmen, und die Ergebnisse archivieren. GuardDuty veröffentlicht diese Metriken CloudWatch unter dem AWS/GuardDuty Namespace bei Amazon.

> ⚠ **GuardDuty zählt übereinstimmende und unterdrückte Ergebnisse unterschiedlich**
>
> GuardDuty wird ausgegeben FindingsMatchedByFilter , wenn ein Ergebnis mit einer Unterdrückungsregel oder einem NOOP-Filter (einem Filter ohne Aktion) übereinstimmt. Diese Metrik wird unabhängig von der Aktion des Filters inkrementiert. GuardDuty wird FindingsSuppressedByFilter nur ausgegeben, wenn die Aktion der Regel Archivieren lautet und es sich bei der Regel um die Archivierungsregel mit der höchsten Priorität für diesen Befund handelt.

GuardDuty veröffentlicht Metriken zur Unterdrückungsregel auf der Grundlage Ihrer Kontokonfiguration:

- Veröffentlicht bei eigenständigen Konten (die nicht Teil einer Organisation sind GuardDuty) Messwerte für dieses Konto.
- Für Konten, die Teil einer Organisation sind, GuardDuty veröffentlicht Metriken auf dem delegierten GuardDuty Administratorkonto. Weitere Informationen zur Funktionsweise von Administrator- und Mitgliedskonten in finden Sie GuardDuty unterMehrere Konten bei Amazon GuardDuty.

Einzelheiten zur Metrik

In der folgenden Tabelle werden die CloudWatch Amazon-Metriken beschrieben, die für Unterdrückungsregeln GuardDuty veröffentlicht werden.

Metrik	Einheit	Description
`FindingsMatchedByFilter`	Anzahl	Die Anzahl der Ergebnisse, die den Kriterien einer Unterdrückungsregel oder eines NOOP-Filters entsprachen. Ein Ergebnis

Metrik	Einheit	Description
		kann mehreren Unterdrüc kungsregeln oder NOOP-Filtern entsprechen und wird pro Treffer einmal GuardDuty gezählt. Jede Übereinstimmung generiert 1 Datenpunkt.
`FindingsSuppressedByFilter`	Anzahl	Die Anzahl der Ergebniss e, die durch eine Unterdrüc kungsregel archiviert wurden. Wenn mehrere Regeln mit demselben Ergebnis übereinst immen, wird nur die Regel mit dem niedrigsten `Rank` Wert GuardDuty gezählt. Bei jeder Unterdrückung wird 1 Datenpunkt generiert.

Metriken zu Unterdrückungsregeln in Amazon anzeigen CloudWatch

Metriken für Unterdrückungsregeln finden Sie in der CloudWatch Amazon-Konsole unter dem AWS/GuardDutyNamespace, gruppiert nach der FilterNameDimension. Der Wert der `FilterName` Dimension ist der Name der Unterdrückungsregel oder des Filters. Anweisungen zur Suche und grafischen Darstellung von Kennzahlen in Amazon CloudWatch finden Sie unter Verfügbare Messwerte anzeigen im CloudWatch Amazon-Benutzerhandbuch.

Anpassen der Bedrohungserkennung mit Entitätenlisten und IP-Adresslisten

Amazon GuardDuty überwacht die Sicherheit Ihrer AWS Umgebung, indem es VPC-Flow-Logs, AWS CloudTrail Event-Logs und DNS-Logs analysiert und verarbeitet. Indem Sie einen oder mehrere spezielle Use-case GuardDuty Schutzpläne (außerLaufzeitüberwachung) aktivieren, können Sie die darin enthaltenen Überwachungsfunktionen erweitern. GuardDuty

Mithilfe von Listen können Sie den Umfang der Bedrohungserkennung in Ihrer Umgebung individuell anpassen. GuardDuty Sie können so konfigurieren GuardDuty , dass keine Ergebnisse mehr aus Ihren vertrauenswürdigen Quellen generiert werden und dass Ergebnisse für bekannte bösartige Quellen aus Ihren Bedrohungslisten generiert werden. GuardDuty unterstützt weiterhin ältere IP-Adresslisten und erweitert die Unterstützung auf Entitätslisten (empfohlen), die IP-Adressen, Domänen oder beides enthalten können.

Themen

- Grundlegendes zu Entitätslisten und IP-Adresslisten
- Wichtige Überlegungen zu GuardDuty Listen
- Listenformate
- Grundlegendes zum Listenstatus
- Voraussetzungen für Entitätslisten und IP-Adresslisten einrichten
- Hinzufügen und Aktivieren einer Entitätsliste oder IP-Liste
- Aktualisierung einer Entitäts- oder IP-Adressliste
- De-activating Entitätsliste oder IP-Adressliste
- Entitätsliste oder IP-Adressliste löschen

Grundlegendes zu Entitätslisten und IP-Adresslisten

GuardDuty bietet zwei Implementierungsansätze: Entitätslisten (empfohlen) und IP-Listen. Beide Methoden helfen Ihnen dabei, vertrauenswürdige Quellen zu spezifizieren, die die Generierung GuardDuty von Erkenntnissen verhindern, und bekannte Bedrohungen, die zur Generierung von Erkenntnissen GuardDuty verwendet werden.

Entitätslisten unterstützen IP-Adressen, Domainnamen und SHA-256 Datei-Hashes. Sie verwenden direkten Zugriff auf Amazon Simple Storage Service (Amazon S3) mit einer einzigen IAM-Berechtigung, die sich nicht auf die Größenbeschränkungen der IAM-Richtlinien in mehreren Regionen auswirkt.

IP-Listen unterstützen nur IP-Adressen und deren Verwendung GuardDuty Serviceverknüpfte Rolle (SLR) (SLR), sodass IAM-Richtlinienaktualisierungen pro Region erforderlich sind, was sich auf die Größenbeschränkungen der IAM-Richtlinien auswirken kann.

Vertrauenswürdige Listen (sowohl Entitätslisten als auch IP-Adresslisten) enthalten Einträge, denen Sie bei der sicheren Kommunikation mit Ihrer Infrastruktur vertrauen. AWS GuardDuty generiert keine

Ergebnisse für Einträge, die in vertrauenswürdigen Quellen aufgeführt sind. Sie können jeweils nur eine Liste vertrauenswürdiger Entitäten und eine Liste vertrauenswürdiger IP-Adressen AWS-Konto pro Region hinzufügen.

Bedrohungslisten (sowohl Entitätslisten als auch IP-Adresslisten) enthalten Einträge, die Sie als bekannte bösartige Quellen identifiziert haben. Wenn eine Aktivität GuardDuty erkannt wird, an der diese Quellen beteiligt sind, generiert es Ergebnisse, die Sie vor potenziellen Sicherheitsproblemen warnen. Sie können Ihre eigenen Bedrohungslisten erstellen oder Feeds mit Bedrohungsinformationen von Drittanbietern integrieren. Diese Liste kann von Bedrohungsdaten von Drittanbietern stammen oder speziell für Ihr Unternehmen erstellt werden. Neben der Generierung von Ergebnissen aufgrund einer potenziell verdächtigen Aktivität werden GuardDuty auch Ergebnisse generiert, die auf einer Aktivität basieren, die Einträge aus Ihren Bedrohungslisten beinhaltet. Sie können jederzeit bis zu sechs Listen mit Bedrohungsentitäten und Bedrohungs-IP-Adressen AWS-Konto pro Region hochladen.

> **Note**
>
> Um von IP-Adresslisten zu Entitätslisten zu migrierenVoraussetzungen für Entitätslisten, folgen Sie den Anweisungen, fügen Sie sie hinzu und aktivieren Sie sie. Danach können Sie wählen, ob Sie die entsprechende IP-Adressliste deaktivieren oder löschen möchten.

Wichtige Überlegungen zu GuardDuty Listen

Bevor Sie mit der Arbeit mit Listen beginnen, sollten Sie die folgenden Überlegungen lesen:

- IP-Adresslisten und Entitätslisten gelten nur für Datenverkehr, der für öffentlich routbare IP-Adressen und Domänen bestimmt ist.
- In einer Entitätsliste gelten die Einträge für VPC Flow Logs in Amazon VPC und Route53 Resolver DNS-Abfrageprotokolle. CloudTrail

  In einer IP-Adressliste beziehen sich die Einträge auf CloudTrail die Ergebnisse von VPC Flow Logs in Amazon VPC, nicht aber auf die Ergebnisse der Route53 Resolver DNS-Abfrageprotokolle.
- Wenn Sie dieselbe IP-Adresse oder Domain sowohl in die Liste der vertrauenswürdigen Adressen als auch in die Liste der Bedrohungen aufnehmen, hat dieser Eintrag in der Liste der vertrauenswürdigen Adressen Vorrang. GuardDuty generiert kein Ergebnis, wenn mit diesem Eintrag eine Aktivität verknüpft ist.

- In einer Umgebung mit mehreren Konten kann nur das GuardDuty Administratorkonto Listen verwalten. Diese Einstellung gilt automatisch für die Mitgliedskonten. GuardDuty generiert Ergebnisse auf der Grundlage einer Aktivität, an der bekannte bösartige IP-Adressen (und Domänen) aus den Bedrohungsquellen des Administratorkontos beteiligt sind, und generiert keine Ergebnisse, die auf Aktivitäten basieren, die IP-Adressen (und Domänen) aus den vertrauenswürdigen Quellen des Administratorkontos betreffen. Weitere Informationen finden Sie unter Mehrere Konten bei Amazon GuardDuty.
- Es werden ausschließlich IPv4-Adressen akzeptiert. IPv6-Adressen werden nicht unterstützt.
- SHA-256 Datei-Hashes werden nur in Listen mit Bedrohungsentitäten unterstützt. Sie können Datei-Hashes nicht in Listen vertrauenswürdiger Entitäten oder IP-Adresslisten aufnehmen.
- Nachdem Sie eine Entitätsliste oder IP-Adressliste aktiviert, deaktiviert oder gelöscht haben, wird der Vorgang voraussichtlich innerhalb von 15 Minuten abgeschlossen sein. In bestimmten Szenarien kann es bis zu 40 Minuten dauern, bis dieser Vorgang abgeschlossen ist.
- GuardDuty verwendet eine Liste nur dann zur Erkennung von Bedrohungen, wenn der Status der Liste Aktiv lautet.
- Jedes Mal, wenn Sie einen Eintrag zum S3-Bucket-Speicherort der Liste hinzufügen oder aktualisieren, müssen Sie die Liste erneut aktivieren. Weitere Informationen finden Sie unter Aktualisierung einer Entitäts- oder IP-Adressliste.
- Entitätslisten und IP-Adressen haben unterschiedliche Kontingente. Weitere Informationen finden Sie unter GuardDuty Kontingente.

Listenformate

GuardDuty akzeptiert mehrere Dateiformate für Ihre Listen und Entitätslisten mit einem Maximum von 35 MB pro Datei. Jedes Format hat spezifische Anforderungen und Funktionen.

Klartext (TXT)

Dieses Format unterstützt IP-Adressen, CIDR-Bereiche, Domainnamen und SHA-256 Datei-Hashes. SHA-256 Datei-Hashes werden nur in Listen mit Bedrohungsentitäten unterstützt. Jeder Eintrag muss in einer separaten Zeile stehen.

Example Beispiel für eine Entitätsliste

```
192.0.2.1
192.0.2.0/24
```

```
example.com
example.org
*.example.org
```

Example Beispiel für eine Liste bedrohlicher Entitäten mit Datei-Hashes

```
192.0.2.1
192.0.2.0/24
example.com
example.org
*.example.org
a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3
```

Example Beispiel für eine IP-Adressliste

```
192.0.2.0/24
198.51.100.1
203.0.113.1
```

Structured Threat Information Expression (STIX)

Dieses Format unterstützt IP-Adressen, CIDR-Block, Domainnamen und SHA-256 Datei-Hashes. STIX ermöglicht es Ihnen, Ihren Bedrohungsinformationen zusätzlichen Kontext hinzuzufügen. GuardDuty verarbeitet IP-Adressen, CIDR-Bereiche, Domainnamen und SHA-256 Datei-Hashes anhand der STIX-Indikatoren. SHA-256 Datei-Hashes werden nur in Listen mit Bedrohungsentitäten unterstützt.

Example Beispiel für eine Entitätsliste

```
<?xml version="1.0" encoding="UTF-8"?>
<stix:STIX_Package
    xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
    xmlns:cybox="http://cybox.mitre.org/cybox-2"
    xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
    xmlns:stix="http://stix.mitre.org/stix-1"
    xmlns:indicator="http://stix.mitre.org/Indicator-2"
    xmlns:stixCommon="http://stix.mitre.org/common-1"
    xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
    xmlns:DomainNameObj="http://cybox.mitre.org/objects#DomainNameObject-1"
    id="example:Package-a1b2c3d4-1111-2222-3333-444455556666"
    version="1.2">
```

```
    <stix:Indicators>
        <stix:Indicator
            id="example:indicator-a1b2c3d4-aaaa-bbbb-cccc-ddddeeeeffff"
            timestamp="2025-08-12T00:00:00Z"
            xsi:type="indicator:IndicatorType"
            xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <indicator:Title>Malicious domain observed Example</indicator:Title>
            <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">Domain
 Watchlist</indicator:Type>
            <indicator:Observable id="example:Observable-0000-1111-2222-3333">
                <cybox:Object id="example:Object-0000-1111-2222-3333">
                    <cybox:Properties xsi:type="DomainNameObj:DomainNameObjectType">
                        <DomainNameObj:Value condition="Equals">bad.example.com</
DomainNameObj:Value>
                    </cybox:Properties>
                </cybox:Object>
            </indicator:Observable>
        </stix:Indicator>
    </stix:Indicators>
</stix:STIX_Package>
```

Example Beispiel für eine Liste bedrohlicher Entitäten mit Datei-Hashes

```
<?xml version="1.0" encoding="UTF-8"?>
<stix:STIX_Package
    xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
    xmlns:cybox="http://cybox.mitre.org/cybox-2"
    xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
    xmlns:stix="http://stix.mitre.org/stix-1"
    xmlns:indicator="http://stix.mitre.org/Indicator-2"
    xmlns:stixCommon="http://stix.mitre.org/common-1"
    xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
    xmlns:DomainNameObj="http://cybox.mitre.org/objects#DomainNameObject-1"
    xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2"
    id="example:Package-a1b2c3d4-1111-2222-3333-444455556666"
    version="1.2">
    <stix:Indicators>
        <stix:Indicator
            id="example:indicator-a1b2c3d4-aaaa-bbbb-cccc-ddddeeeeffff"
            timestamp="2025-08-12T00:00:00Z"
            xsi:type="indicator:IndicatorType"
            xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <indicator:Title>Malicious domain observed Example</indicator:Title>
```

```
            <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">Domain
 Watchlist</indicator:Type>
            <indicator:Observable id="example:Observable-0000-1111-2222-3333">
                <cybox:Object id="example:Object-0000-1111-2222-3333">
                    <cybox:Properties xsi:type="DomainNameObj:DomainNameObjectType">
                        <DomainNameObj:Value condition="Equals">bad.example.com</
DomainNameObj:Value>
                    </cybox:Properties>
                </cybox:Object>
            </indicator:Observable>
        </stix:Indicator>
        <stix:Indicator
            id="example:indicator-a1b2c3d4-eeee-ffff-0000-111122223333"
            timestamp="2025-08-12T00:00:00Z"
            xsi:type="indicator:IndicatorType"
            xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <indicator:Title>File hash for malware variant</indicator:Title>
            <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">File Hash
 Watchlist</indicator:Type>
            <indicator:Observable id="example:Observable-4444-5555-6666-7777">
                <cybox:Object id="example:File-4444-5555-6666-7777">
                    <cybox:Properties xsi:type="FileObj:FileObjectType">
                        <FileObj:Hashes>
                            <cyboxCommon:Hash>
                                <cyboxCommon:Type
 xsi:type="cyboxVocabs:HashNameVocab-1.0">SHA256</cyboxCommon:Type>
                                <cyboxCommon:Simple_Hash_Value
 condition="Equals">a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3</
cyboxCommon:Simple_Hash_Value>
                            </cyboxCommon:Hash>
                        </FileObj:Hashes>
                    </cybox:Properties>
                </cybox:Object>
            </indicator:Observable>
        </stix:Indicator>
    </stix:Indicators>
</stix:STIX_Package>
```

Example Beispiel für eine IP-Adressliste

```
<?xml version="1.0" encoding="UTF-8"?>
<stix:STIX_Package
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
    xmlns:stix="http://stix.mitre.org/stix-1"
    xmlns:stixCommon="http://stix.mitre.org/common-1"
    xmlns:ttp="http://stix.mitre.org/TTP-1"
    xmlns:cybox="http://cybox.mitre.org/cybox-2"
    xmlns:AddressObject="http://cybox.mitre.org/objects#AddressObject-2"
    xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
    xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
    xmlns:example="http://example.com/"
    xsi:schemaLocation="
    http://stix.mitre.org/stix-1 http://stix.mitre.org/XMLSchema/core/1.2/
stix_core.xsd
    http://stix.mitre.org/Campaign-1 http://stix.mitre.org/XMLSchema/campaign/1.2/
campaign.xsd
    http://stix.mitre.org/Indicator-2 http://stix.mitre.org/XMLSchema/indicator/2.2/
indicator.xsd
    http://stix.mitre.org/TTP-2 http://stix.mitre.org/XMLSchema/ttp/1.2/ttp.xsd
    http://stix.mitre.org/default_vocabularies-1 http://stix.mitre.org/XMLSchema/
default_vocabularies/1.2.0/stix_default_vocabularies.xsd
    http://cybox.mitre.org/objects#AddressObject-2 http://cybox.mitre.org/XMLSchema/
objects/Address/2.1/Address_Object.xsd"
    id="example:STIXPackage-a78fc4e3-df94-42dd-a074-6de62babfe16"
    version="1.2">
    <stix:Observables cybox_major_version="1" cybox_minor_version="1">
        <cybox:Observable id="example:observable-80b26f43-
dc41-43ff-861d-19aff31e0236">
            <cybox:Object id="example:object-161a5438-1c26-4275-ba44-a35ba963c245">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">

 <AddressObject:Address_Valuecondition="InclusiveBetween">192.0.2.0##comma##192.0.2.255</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
        <cybox:Observable id="example:observable-b442b399-aea4-436f-bb34-
b9ef6c5ed8ab">
            <cybox:Object id="example:object-b422417f-bf78-4b34-ba2d-de4b09590a6d">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">
                    <AddressObject:Address_Value>198.51.100.1</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
```

```
        <cybox:Observable
 id="example:observable-1742fa06-8b5e-4449-9d89-6f9f32595784">
            <cybox:Object id="example:object-dc73b749-8a31-46be-803f-71df77565391">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">
                    <AddressObject:Address_Value>203.0.113.1</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
    </stix:Observables>
</stix:STIX_Package>
```

Open Threat Exchange (OTX)™ CSV

Dieses Format unterstützt den CIDR-Block, einzelne IP-Adressen, Domänen und den SHA256 Indikatortyp für Datei-Hashes. SHA-256 Datei-Hashes werden nur in Listen mit Bedrohungsentitäten unterstützt. Dieses Dateiformat hat kommagetrennte Werte.

Example Beispiel für eine Entitätsliste

```
Indicator type, Indicator, Description
CIDR, 192.0.2.0/24, example
IPv4, 198.51.100.1, example
IPv4, 203.0.113.1, example
Domain name, example.net, example
```

Example Beispiel für eine Liste bedrohlicher Entitäten mit Datei-Hashes

```
Indicator type, Indicator, Description
CIDR, 192.0.2.0/24, example
IPv4, 198.51.100.1, example
IPv4, 203.0.113.1, example
Domain name, example.net, example
SHA256, a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3, example
```

Example Beispiel für eine IP-Adressliste

```
Indicator type, Indicator, Description
CIDR, 192.0.2.0/24, example
```

```
IPv4, 198.51.100.1, example
IPv4, 203.0.113.1, example
```

FireEye™ iSight Threat Intelligence CSV

Dieses Format unterstützt den CIDR-Block, einzelne IP-Adressen, Domänen und SHA-256 Datei-Hashes in der Spalte. `sha256` SHA-256 Datei-Hashes werden nur in Listen mit Bedrohungsentitäten unterstützt. Die folgenden Beispiellisten verwenden ein `FireEye™` CSV-Format.

Example Beispiel für eine Entitätsliste

```
reportId, title, threatScape, audience, intelligenceType, publishDate, reportLink,
 webLink, emailIdentifier, senderAddress, senderName, sourceDomain, sourceIp, subject,
 recipient, emailLanguage, fileName, fileSize, fuzzyHash, fileIdentifier, md5, sha1,
 sha256, description, fileType, packer, userAgent, registry, fileCompilationDateTime,
 filePath, asn, cidr, domain, domainTimeOfLookup, networkIdentifier, ip, port,
 protocol, registrantEmail, registrantName, networkType, url, malwareFamily,
 malwareFamilyId, actor, actorId, observationTime

01-00000001, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000001, https://www.example.com/
report/01-00000001, , , , , , , , , , , , , , , , , , , , , , , , , 192.0.2.0/24, , ,
 Related, , , , , , network, , Ursnif, 21a14673-0d94-46d3-89ab-8281a0466099, , ,
 1494944400

01-00000002, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000002, https://www.example.com/
report/01-00000002, , , , , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 198.51.100.1, , , , , network, , Ursnif,
 12ab7bc4-62ed-49fa-99e3-14b92afc41bf, , ,1494944400

01-00000003, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000003, https://www.example.com/
report/01-00000003, , , , , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 203.0.113.1, , , , , network, , Ursnif, 8a78c3db-7bcb-40bc-a080-75bd35a2572d, , ,
 1494944400

 01-00000002, Malicious domain observed in test, Test, Operational, threat,
 1494944400, https://www.example.com/report/01-00000002,https://www.example.com/
report/01-00000002,,,,,,,,,,,,,,,,,,,,,,, 203.0.113.0/24, example.com,, Related,
 203.0.113.0, 8080, UDP,,, network,, Ursnif, fc13984c-c767-40c9-8329-f4c59557f73b,,,
 1494944400
```

Example Beispiel für eine Liste bedrohlicher Entitäten mit Datei-Hashes

```
reportId, title, threatScape, audience, intelligenceType, publishDate, reportLink,
 webLink, emailIdentifier, senderAddress, senderName, sourceDomain, sourceIp, subject,
 recipient, emailLanguage, fileName, fileSize, fuzzyHash, fileIdentifier, md5, sha1,
 sha256, description, fileType, packer, userAgent, registry, fileCompilationDateTime,
 filePath, asn, cidr, domain, domainTimeOfLookup, networkIdentifier, ip, port,
 protocol, registrantEmail, registrantName, networkType, url, malwareFamily,
 malwareFamilyId, actor, actorId, observationTime

01-00000001, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000001, https://www.example.com/
report/01-00000001, , , , , , , , , , , , , , , , , , , , , , , , , , , , , 192.0.2.0/24, , ,
 Related, , , , , , network, , Ursnif, 21a14673-0d94-46d3-89ab-8281a0466099, , ,
 1494944400

01-00000002, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000002, https://www.example.com/
report/01-00000002, , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 198.51.100.1, , , , , network, , Ursnif,
 12ab7bc4-62ed-49fa-99e3-14b92afc41bf, , ,1494944400

01-00000003, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000003, https://www.example.com/
report/01-00000003, , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 203.0.113.1, , , , , network, , Ursnif, 8a78c3db-7bcb-40bc-a080-75bd35a2572d, , ,
 1494944400

 01-00000002, Malicious domain observed in test, Test, Operational, threat,
 1494944400, https://www.example.com/report/01-00000002,https://www.example.com/
report/01-00000002,,,,,,,,,,,,,,,,,,,,,,,, 203.0.113.0/24, example.com,, Related,
 203.0.113.0, 8080, UDP,,, network,, Ursnif, fc13984c-c767-40c9-8329-f4c59557f73b,,,
 1494944400

01-00000005, Malicious file hash, Test, Operational, threat,
 1494944400, https://www.example.com/report/01-00000005, https://
www.example.com/report/01-00000005, , , , , , , , , , , , , , , ,
 a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3, , , , , , , , , , , ,
 Related, , , , , , network, , Ursnif, 9b9a6ea0-3cbf-4e12-bd3e-0c1d7b4e5f6a, , ,
 1494944400
```

Example Beispiel für eine IP-Adressliste

```
reportId, title, threatScape, audience, intelligenceType, publishDate, reportLink,
 webLink, emailIdentifier, senderAddress, senderName, sourceDomain, sourceIp, subject,
 recipient, emailLanguage, fileName, fileSize, fuzzyHash, fileIdentifier, md5, sha1,
 sha256, description, fileType, packer, userAgent, registry, fileCompilationDateTime,
 filePath, asn, cidr, domain, domainTimeOfLookup, networkIdentifier, ip, port,
 protocol, registrantEmail, registrantName, networkType, url, malwareFamily,
 malwareFamilyId, actor, actorId, observationTime

01-00000001, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000001, https://www.example.com/
report/01-00000001, , , , , , , , , , , , , , , , , , , , , , , , , 192.0.2.0/24, , ,
 Related, , , , , , network, , Ursnif, 21a14673-0d94-46d3-89ab-8281a0466099, , ,
 1494944400

01-00000002, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000002, https://www.example.com/
report/01-00000002, , , , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 198.51.100.1, , , , , network, , Ursnif,
 12ab7bc4-62ed-49fa-99e3-14b92afc41bf, , ,1494944400

01-00000003, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000003, https://www.example.com/
report/01-00000003, , , , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 203.0.113.1, , , , , network, , Ursnif, 8a78c3db-7bcb-40bc-a080-75bd35a2572d, , ,
 1494944400
```

Proofpoint™ ET Intelligence Feed CSV

Im ProofPoint CSV-Format können Sie entweder IP-Adressen oder Domainnamen zu einer einzigen Liste hinzufügen. Die folgende Beispielliste verwendet das `Proofpoint`-CSV-Format. Die Angabe eines Werts für den `ports` Parameter ist optional. Wenn Sie ihn nicht angeben, hinterlassen Sie am Ende ein Komma (,).

Example Beispiel für eine Entitätsliste

```
domain, category, score, first_seen, last_seen, ports (|)
198.51.100.1, 1, 100, 2000-01-01, 2000-01-01,
203.0.113.1, 1, 100, 2000-01-01, 2000-01-01, 80
```

Example Beispiel für eine IP-Adressliste

```
ip, category, score, first_seen, last_seen, ports (|)
198.51.100.1, 1, 100, 2000-01-01, 2000-01-01,
203.0.113.1, 1, 100, 2000-01-01, 2000-01-01, 80
```

AlienVault™ Reputation Feed

Die folgende Beispielliste verwendet das `AlienVault`-Format. Dieses Format unterstützt auch SHA-256 Datei-Hashes in der Indikatorspalte. SHA-256 Datei-Hashes werden nur in Listen mit Bedrohungsentitäten unterstützt.

Example Beispiel für eine Entitätsliste

```
192.0.2.1#4#2#Malicious Host#KR##37.5111999512,126.974098206#3
192.0.2.2#4#2#Scanning Host#IN#Gurgaon#28.4666996002,77.0333023071#3
192.0.2.3#4#2##CN#Guangzhou#23.1166992188,113.25#3
www.test.org#4#2#Malicious Host#CA#Brossard#45.4673995972,-73.4832000732#3
www.example.com#4#2#Malicious Host#PL##52.2393989563,21.0361995697#3
```

Example Beispiel für eine Liste bedrohlicher Entitäten mit Datei-Hashes

```
192.0.2.1#4#2#Malicious Host#KR##37.5111999512,126.974098206#3
192.0.2.2#4#2#Scanning Host#IN#Gurgaon#28.4666996002,77.0333023071#3
192.0.2.3#4#2##CN#Guangzhou#23.1166992188,113.25#3
www.test.org#4#2#Malicious Host#CA#Brossard#45.4673995972,-73.4832000732#3
www.example.com#4#2#Malicious Host#PL##52.2393989563,21.0361995697#3
a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3#4#2#Malicious
 Hash###0.0,0.0#3
```

Example Beispiel für eine IP-Adressliste

```
198.51.100.1#4#2#Malicious Host#US##0.0,0.0#3
203.0.113.1#4#2#Malicious Host#US##0.0,0.0#3
```

Grundlegendes zum Listenstatus

Wenn Sie eine Entitätsliste oder eine IP-Adressliste hinzufügen, GuardDuty wird der Status dieser Liste angezeigt. Die Spalte Status gibt an, ob die Liste wirksam ist und ob Maßnahmen erforderlich sind. In der folgenden Liste werden gültige Statuswerte beschrieben:

- Aktiv — Zeigt an, dass die Liste derzeit für die Erkennung benutzerdefinierter Bedrohungen verwendet wird.
- Inaktiv — Zeigt an, dass die Liste derzeit nicht verwendet wird. Informationen GuardDuty zur Verwendung dieser Liste zur Erkennung von Bedrohungen in Ihrer Umgebung finden Sie unter Schritt 3: Aktivieren einer Entitäts- oder IP-Adressliste in[Hinzufügen und Aktivieren einer Entitätsliste oder IP-Liste](#).
- Fehler — Zeigt an, dass ein Problem mit der Liste vorliegt. Bewegen Sie den Mauszeiger über den Status, um die Fehlerdetails anzuzeigen.
- Aktiviert — Zeigt an, GuardDuty dass der Vorgang zur Aktivierung der Liste eingeleitet wurde. Sie können den Status dieser Liste weiter überwachen. Wenn kein Fehler auftritt, sollte der Status auf Aktiv aktualisiert werden. Solange der Status Aktiviert bleibt, können Sie in dieser Liste keine Aktion ausführen. Es kann einige Minuten dauern, bis sich der Status der Liste auf Aktiv ändert.
- Deaktiviert — Zeigt an, GuardDuty dass der Prozess der Deaktivierung der Liste eingeleitet wurde. Sie können den Status dieser Liste weiter überwachen. Wenn kein Fehler vorliegt, sollte der Status auf Inaktiv aktualisiert werden. Solange der Status Deaktiviert bleibt, können Sie in dieser Liste keine Aktion ausführen.
- Ausstehend löschen — Zeigt an, dass die Liste gerade gelöscht wird. Solange der Status „Ausstehend löschen“ bleibt, können Sie für diese Liste keine Aktion ausführen.

Voraussetzungen für Entitätslisten und IP-Adresslisten einrichten

GuardDuty verwendet Entitätslisten und IP-Adresslisten, um die Bedrohungserkennung in Ihrer AWS Umgebung individuell anzupassen. Entitätslisten (empfohlen) unterstützen sowohl IP-Adressen als auch Domainnamen, während IP-Adresslisten nur IP-Adressen unterstützen. Bevor Sie mit der Erstellung dieser Listen beginnen, müssen Sie die erforderlichen Berechtigungen für den Listentyp hinzufügen, den Sie verwenden möchten.

Voraussetzungen für Entitätslisten

GuardDuty Liest beim Hinzufügen von Entitätslisten Ihre vertrauenswürdigen Listen und Listen mit Bedrohungsinformationen aus S3-Buckets. Die Rolle, die Sie zum Erstellen von Entitätslisten verwenden, muss über die `s3:GetObject` Berechtigung für die S3-Buckets verfügen, die diese Listen enthalten.

> **Note**
>
> In einer Umgebung mit mehreren Konten kann nur das GuardDuty Administratorkonto Listen verwalten, die automatisch für Mitgliedskonten gelten.

Wenn Sie noch nicht über die `s3:GetObject` Berechtigung für den S3-Bucket-Standort verfügen, verwenden Sie die folgende Beispielrichtlinie und *`amzn-s3-demo-bucket`* ersetzen Sie sie durch Ihren S3-Bucket-Standort.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/[object-key]"
        }
    ]
}
```

Voraussetzungen für IP-Adresslisten

Verschiedene IAM-Identitäten erfordern spezielle Berechtigungen, um mit vertrauenswürdigen IP-Listen und Bedrohungslisten in arbeiten zu können. GuardDuty Eine Identität, der die verwaltete Richtlinie AmazonGuardDutyFullAccess_v2 (empfohlen) angefügt ist, kann nur hochgeladene Listen mit vertrauenswürdigen IPs und Bedrohungslisten umbenennen und deaktivieren.

Um verschiedenen Identitäten vollen Zugriff auf die Arbeit mit vertrauenswürdigen IP-Listen und Bedrohungslisten zu erteilen (dies umfasst neben dem Umbenennen und Deaktivieren auch das Hinzufügen, Aktivieren, Löschen und Aktualisieren des Speicherorts oder der Namen der Listen), stellen Sie sicher, dass die folgenden Aktionen in der einem Benutzer, einer Gruppe oder einer Rolle zugewiesenen Berechtigungsrichtlinie vorhanden sind:

```
{
    "Effect": "Allow",
```

```
    "Action": [
        "iam:PutRolePolicy",
        "iam:DeleteRolePolicy"
    ],
    "Resource": "arn:aws:iam::555555555555:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
}
```

> **Important**
>
> Diese Aktionen sind nicht in der verwalteten Richtlinie `AmazonGuardDutyFullAccess` enthalten.

SSE-KMS Verschlüsselung mit Entitätslisten und IP-Listen verwenden

GuardDuty unterstützt SSE-AES256 und SSE-KMS verschlüsselt Ihre Listen. SSE-C wird nicht unterstützt. Weitere Informationen zu Verschlüsselungstypen für S3 finden Sie unter Schützen von Daten mithilfe serverseitiger Verschlüsselung.

Unabhängig davon, ob Sie Entitätslisten oder IP-Listen verwenden SSE-KMS, fügen Sie Ihrer AWS KMS key Richtlinie die folgende Anweisung hinzu, falls Sie diese verwenden. *123456789012*Ersetzen Sie es durch Ihre eigene Konto-ID.

```
{
    "Sid": "AllowGuardDutyServiceRole",
    "Effect": "Allow",
    "Principal": {
    "AWS": "arn:aws:iam::123456789012:role/aws-service-role/guardduty.amazonaws.com/
AWSServiceRoleForAmazonGuardDuty"
    },
    "Action": "kms:Decrypt*",
    "Resource": "*"
}
```

Hinzufügen und Aktivieren einer Entitätsliste oder IP-Liste

Entitätslisten und IP-Adresslisten helfen Ihnen dabei, die Funktionen zur Bedrohungserkennung in anzupassen GuardDuty. Weitere Informationen zu diesen Listen finden Sie unterGrundlegendes zu Entitätslisten und IP-Adresslisten. Es GuardDuty empfiehlt, Entitätslisten zu verwenden, um die

vertrauenswürdigen Daten und Bedrohungsinformationen für Ihre AWS Umgebung zu verwalten. Bevor Sie beginnen, sehen Sie sich Voraussetzungen für Entitätslisten und IP-Adresslisten einrichten an.

Wählen Sie eine der folgenden Zugriffsmethoden, um eine Liste vertrauenswürdiger Entitäten, Bedrohungsentitäten, vertrauenswürdiger IP-Adressen oder eine Liste mit Bedrohungs-IP-Adressen hinzuzufügen und zu aktivieren.

Console

(Optional) Schritt 1: Den Standort-URL Ihrer Liste abrufen

1. Öffnen Sie die Amazon S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie im Navigationsbereich die Option Buckets aus.
3. Wählen Sie den Amazon-S3-Bucket-Namen, der die spezifische Liste enthält, die Sie hinzufügen möchten.
4. Wählen Sie den Namen des Objekts (Liste), um dessen Details anzuzeigen.
5. Kopieren Sie auf der Registerkarte Eigenschaften den S3-URI für dieses Objekt.

Schritt 2: Hinzufügen vertrauenswürdiger Daten oder Daten zur Bedrohungsanalyse

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Listen.
3. Wählen Sie auf der Seite Listen die Registerkarte Entitätslisten oder IP-Adresslisten aus.
4. Wählen Sie je nach ausgewähltem Tab, ob Sie eine Vertrauensliste oder eine Bedrohungsliste hinzufügen möchten.
5. Gehen Sie im Dialogfeld zum Hinzufügen einer Vertrauens- oder einer Bedrohungsliste wie folgt vor:

   a. In Name der Liste geben Sie einen Namen für Ihre Liste ein.

      Einschränkungen bei der Benennung von Listen — Der Name Ihrer Liste kann Kleinbuchstaben, Großbuchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten.

      Bei einer IP-Adressliste muss der Name Ihrer Liste innerhalb einer AWS-Konto UND-Region eindeutig sein.

b. Geben Sie unter Standort den Ort an, an dem Sie Ihre Liste hochgeladen haben. Falls Sie den Standort noch nicht haben, finden Sie weitere Informationen unter Step 1: Fetching location URL of your list.

   Gilt nur für benutzerdefinierte Gruppen von Bedrohungen und benutzerdefinierten vertrauenswürdigen Entitäten — Wenn Sie eine Standort-URL angeben, die nicht den folgenden unterstützten Formaten entspricht, erhalten Sie beim Hinzufügen und Aktivieren der Liste eine Fehlermeldung.

   Format der Standort-URL:

   - https://s3.amazonaws.com/bucket.name/file.txt
   - https://s3-aws-region.amazonaws.com/bucket.name/file.txt
   - http://bucket.s3.amazonaws.com/file.txt
   - http://bucket.s3-aws-region.amazonaws.com/file.txt
   - s3://bucket. name/file.txt

c. (Optional) Für den erwarteten Bucket-Besitzer können Sie die AWS-Konto ID eingeben, der der Amazon S3-Bucket gehört, der im Feld Standort angegeben ist.

   Wenn Sie keinen AWS-Konto ID-Besitzer angeben, GuardDuty verhält sich das für Entitätslisten und IP-Adresslisten unterschiedlich. Bei Entitätslisten GuardDuty wird überprüft, ob das aktuelle Mitgliedskonto den im Feld Standort angegebenen S3-Bucket besitzt. Wenn Sie bei IP-Adresslisten keinen AWS-Konto ID-Besitzer angeben, GuardDuty wird keine Überprüfung durchgeführt.

   Wenn GuardDuty festgestellt wird, dass dieser S3-Bucket nicht zur angegebenen Konto-ID gehört, erhalten Sie bei der Aktivierung der Liste eine Fehlermeldung.

d. Aktivieren Sie das Kontrollkästchen I agree.

e. Wählen Sie Liste hinzufügen. Standardmäßig ist der Status der hinzugefügten Liste Inaktiv. Damit die Liste gültig ist, müssen Sie sie aktivieren.

Schritt 3: Aktivierung einer Entitäts- oder IP-Adressliste

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Listen.

3. Wählen Sie auf der Seite Listen die Registerkarte aus, auf der Sie die Liste aktivieren möchten — Entitätslisten oder IP-Adresslisten.
4. Wählen Sie eine Liste aus, die Sie aktivieren möchten. Dadurch werden das Menü Aktion und Bearbeiten aktiviert.
5. Wählen Sie Aktion und dann Aktivieren.

API/CLI

Um eine Liste vertrauenswürdiger Entitäten hinzuzufügen und zu aktivieren

1. Führen Sie CreateTrustedEntitySet. Stellen Sie sicher, dass Sie das `detectorId` Mitgliedskonto angeben, für das Sie diese Liste vertrauenswürdiger Entitäten erstellen möchten. Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

   Einschränkungen bei der Benennung von Listen — Der Name Ihrer Liste kann Kleinbuchstaben, Großbuchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten.
2. Alternativ können Sie dies tun, indem Sie den folgenden Befehl ausführen: AWS Command Line Interface

   ```
   aws guardduty create-trusted-entity-set \
   --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
   --name "AnyOrganizationListEXAMPLE" \
   --format TXT \
   --location "https://s3.amazonaws.com/amzn-s3-demo-bucket/DOC-EXAMPLE-SOURCE-FILE.format" \
   --activate
   ```

   `detector-id`Ersetzen Sie durch die Detektor-ID des Mitgliedskontos, für das Sie die Liste der vertrauenswürdigen Entitäten erstellen werden, sowie durch andere Platzhalterwerte, die *shown in red*

   Wenn Sie diese neu erstellte Liste nicht aktivieren möchten, ersetzen Sie den Parameter `--activate` durch`--no-activate`.

   Der Parameter `expected-bucket-owner` ist optional. Unabhängig davon, ob Sie den Wert für diesen Parameter angeben oder nicht, wird GuardDuty bestätigt, dass die diesem

`--detector-id` Wert zugeordnete AWS-Konto ID den im `--location` Parameter angegebenen S3-Bucket besitzt. Wenn GuardDuty festgestellt wird, dass dieser S3-Bucket nicht zur angegebenen Konto-ID gehört, erhalten Sie bei der Aktivierung dieser Liste eine Fehlermeldung.

Gilt nur für benutzerdefinierte Gruppen von Bedrohungen und benutzerdefinierten vertrauenswürdigen Entitäten — Wenn Sie eine Standort-URL angeben, die nicht den folgenden unterstützten Formaten entspricht, erhalten Sie beim Hinzufügen und Aktivieren der Liste eine Fehlermeldung.

So fügen Sie Listen mit Bedrohungsentitäten hinzu und aktivieren sie

1. Führen Sie CreateThreatEntitySet. Stellen Sie sicher, dass Sie das `detectorId` Mitgliedskonto angeben, für das Sie diese Liste der Bedrohungsentitäten erstellen möchten. Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

   Einschränkungen bei der Benennung von Listen — Der Name Ihrer Liste kann Kleinbuchstaben, Großbuchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten.

2. Alternativ können Sie dies tun, indem Sie den folgenden Befehl ausführen: AWS Command Line Interface

   ```
   aws guardduty create-threat-entity-set \
   --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
   --name "AnyOrganizationListEXAMPLE" \
   --format TXT \
   --location "https://s3.amazonaws.com/amzn-s3-demo-bucket/DOC-EXAMPLE-SOURCE-FILE.format" \
   --activate
   ```

   `detector-id`Ersetzen Sie durch die Detektor-ID des Mitgliedskontos, für das Sie die Liste der vertrauenswürdigen Entitäten erstellen werden, sowie durch andere Platzhalterwerte, die *`shown in red`*

   Wenn Sie diese neu erstellte Liste nicht aktivieren möchten, ersetzen Sie den Parameter `--activate` durch`--no-activate`.

Der Parameter `expected-bucket-owner` ist optional. Unabhängig davon, ob Sie den Wert für diesen Parameter angeben oder nicht, wird GuardDuty bestätigt, dass die diesem `--detector-id` Wert zugeordnete AWS-Konto ID den im `--location` Parameter angegebenen S3-Bucket besitzt. Wenn GuardDuty festgestellt wird, dass dieser S3-Bucket nicht zur angegebenen Konto-ID gehört, erhalten Sie bei der Aktivierung dieser Liste eine Fehlermeldung.

Gilt nur für benutzerdefinierte Gruppen von Bedrohungen und benutzerdefinierten vertrauenswürdigen Entitäten — Wenn Sie eine Standort-URL angeben, die nicht den folgenden unterstützten Formaten entspricht, erhalten Sie beim Hinzufügen und Aktivieren der Liste eine Fehlermeldung.

So fügen Sie eine Liste vertrauenswürdiger IP-Adressen hinzu und aktivieren sie

1. Führen Sie CreateIPSet aus. Stellen Sie sicher, dass Sie das Mitgliedskonto angeben, für das Sie diese Liste vertrauenswürdiger IP-Adressen erstellen möchten. `detectorId` Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

   Bei einer IP-Adressliste muss der Name Ihrer Liste innerhalb einer AWS-Konto UND-Region eindeutig sein.

   Einschränkungen bei der Benennung von Listen — Der Name Ihrer Liste kann Kleinbuchstaben, Großbuchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten.

2. Sie können dies auch tun, indem Sie den folgenden AWS Command Line Interface Befehl ausführen und sicherstellen, dass Sie den durch die `detector-id` Detektor-ID des Mitgliedskontos ersetzen, für das Sie die Liste der vertrauenswürdigen IP-Adressen aktualisieren werden.

```
aws guardduty create-ip-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--name "AnyOrganizationListEXAMPLE" \
--format TXT \
--location "https://s3.amazonaws.com/amzn-s3-demo-bucket/DOC-EXAMPLE-SOURCE-FILE.format" \
--activate
```

`detector-id`Ersetzen Sie es durch die Detektor-ID des Mitgliedskontos, für das Sie die Liste der vertrauenswürdigen IP-Adressen erstellen werden, und durch andere Platzhalterwerte, die vorhanden sind*shown in red*.

Wenn Sie diese neu erstellte Liste nicht aktivieren möchten, ersetzen Sie den Parameter `--activate` durch`--no-activate`.

Der Parameter `expected-bucket-owner` ist optional. Wenn Sie die Konto-ID, der der S3-Bucket gehört, GuardDuty nicht angeben, wird keine Validierung durchgeführt. Wenn Sie die Konto-ID für den `expected-bucket-owner` Parameter angeben, wird GuardDuty überprüft, ob diese AWS-Konto ID Eigentümer des im `--location` Parameter angegebenen S3-Bucket ist. Wenn GuardDuty festgestellt wird, dass dieser S3-Bucket nicht zur angegebenen Konto-ID gehört, erhalten Sie bei der Aktivierung dieser Liste eine Fehlermeldung.

Um IP-Listen für Bedrohungen hinzuzufügen und zu aktivieren

1. Führen Sie CreateThreatIntelSet. Stellen Sie sicher, dass Sie das `detectorId` Mitgliedskonto angeben, für das Sie diese Bedrohungs-IP-Adressliste erstellen möchten. Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

   Einschränkungen bei der Benennung von Listen — Der Name Ihrer Liste kann Kleinbuchstaben, Großbuchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten.

   Bei einer IP-Adressliste muss der Name Ihrer Liste innerhalb einer AWS-Konto UND-Region eindeutig sein.
2. Sie können dies auch tun, indem Sie den folgenden AWS Command Line Interface Befehl ausführen und sicherstellen, dass Sie die durch die `detector-id` Detektor-ID des Mitgliedskontos ersetzen, für das Sie die Liste der Bedrohungs-IP-Adressen aktualisieren.

```
aws guardduty create-threat-intel-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--name "AnyOrganizationListEXAMPLE" \
--format TXT \
--location "https://s3.amazonaws.com/amzn-s3-demo-bucket/DOC-EXAMPLE-SOURCE-FILE.format" \
--activate
```

`detector-id`Ersetzen Sie es durch die Detektor-ID des Mitgliedskontos, für das Sie die Bedrohungs-IP-Liste erstellen werden, und durch andere Platzhalterwerte, die vorhanden sind*shown in red*.

Wenn Sie diese neu erstellte Liste nicht aktivieren möchten, ersetzen Sie den Parameter `--activate` durch`--no-activate`.

Der Parameter `expected-bucket-owner` ist optional. Wenn Sie die Konto-ID, der der S3-Bucket gehört, GuardDuty nicht angeben, wird keine Validierung durchgeführt. Wenn Sie die Konto-ID für den `expected-bucket-owner` Parameter angeben, wird GuardDuty überprüft, ob diese AWS-Konto ID Eigentümer des im `--location` Parameter angegebenen S3-Bucket ist. Wenn GuardDuty festgestellt wird, dass dieser S3-Bucket nicht zur angegebenen Konto-ID gehört, erhalten Sie bei der Aktivierung dieser Liste eine Fehlermeldung.

Nachdem Sie eine Entitätsliste oder IP-Adressliste aktiviert haben, kann es einige Minuten dauern, bis diese Liste wirksam wird. Weitere Informationen finden Sie unter Wichtige Überlegungen zu GuardDuty Listen.

Aktualisierung einer Entitäts- oder IP-Adressliste

Mit Entitätslisten und IP-Adresslisten können Sie die Funktionen zur Bedrohungserkennung in anpassen GuardDuty. Weitere Informationen zu diesen Listen finden Sie unterGrundlegendes zu Entitätslisten und IP-Adresslisten.

Sie können den Namen einer Liste, den S3-Bucket-Speicherort, die erwartete Account-ID des Bucket-Besitzers und die Einträge in einer vorhandenen Liste aktualisieren. Wenn Sie die Einträge in einer Liste aktualisieren, müssen Sie die Schritte zum erneuten Aktivieren der Liste ausführen GuardDuty , um die neueste Version der Liste verwenden zu können. Nachdem Sie eine Entitätsliste oder IP-Adressliste aktualisiert oder aktiviert haben, kann es einige Minuten dauern, bis diese Liste wirksam wird. Weitere Informationen finden Sie unter Wichtige Überlegungen zu GuardDuty Listen.

> **Note**
>
> Wenn der Status einer Liste Aktiviert, Deaktiviert oder Ausstehend löschen lautet, müssen Sie einige Minuten warten, bevor Sie eine Aktion ausführen. Informationen zu diesen Status finden Sie unter. Grundlegendes zum Listenstatus

Wählen Sie eine der Zugriffsmethoden, um eine Entitäts- oder IP-Adressliste zu aktualisieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Listen.
3. Wählen Sie auf der Listenseite die entsprechende Registerkarte — Entitätslisten oder IP-Adresslisten.
4. Wählen Sie eine Liste (vertrauenswürdig oder bedrohlich) aus, die Sie aktualisieren möchten. Dadurch werden die Menüs Aktion und Bearbeiten aktiviert.
5. Wählen Sie Bearbeiten aus.
6. Geben Sie im Dialogfeld zum Aktualisieren der Liste die Details an, die Sie aktualisieren möchten.

   Einschränkungen bei der Benennung von Listen — Der Name Ihrer Liste kann Kleinbuchstaben, Großbuchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten.

   Bei einer IP-Adressliste muss der Name Ihrer Liste innerhalb einer AWS-Konto UND-Region eindeutig sein.

   Gilt nur für benutzerdefinierte Bedrohungsgruppen und benutzerdefinierte Gruppen vertrauenswürdiger Entitäten — Wenn Sie eine Standort-URL angeben, die nicht den folgenden unterstützten Formaten entspricht, erhalten Sie beim Hinzufügen und Aktivieren der Liste eine Fehlermeldung.
7. (Optional) Für Erwarteter Bucket-Besitzer können Sie die AWS-Konto ID eingeben, der der Amazon S3 S3-Bucket gehört, der im Feld Standort angegeben ist.

   Wenn Sie keinen AWS-Konto ID-Besitzer angeben, GuardDuty verhält sich das Verhalten bei Entitätslisten und IP-Adresslisten unterschiedlich. GuardDuty Überprüft bei Entitätslisten, ob das aktuelle Mitgliedskonto Eigentümer des im Feld Standort angegebenen S3-Buckets ist. Wenn Sie bei IP-Adresslisten keinen AWS-Konto ID-Besitzer angeben, GuardDuty wird keine Überprüfung durchgeführt.

   Wenn GuardDuty festgestellt wird, dass dieser S3-Bucket nicht zur angegebenen Konto-ID gehört, erhalten Sie bei der Aktivierung der Liste eine Fehlermeldung.
8. Aktivieren Sie das Kontrollkästchen Ich stimme zu und wählen Sie dann Liste aktualisieren aus.

API/CLI

Um mit den folgenden Verfahren zu beginnen, benötigen Sie die ID, z. B.`trustedEntitySetId`, `threatEntitySetIdtrustedIpSet`, oder`threatIpSet`, die der Listenressource zugeordnet ist, die Sie aktualisieren möchten.

Um eine Liste vertrauenswürdiger Entitäten zu aktualisieren und zu aktivieren

1. Führen Sie UpdateTrustedEntitySet. Stellen Sie sicher, dass Sie das `detectorId` Mitgliedskonto angeben, für das Sie diese Liste der vertrauenswürdigen Entitäten aktualisieren möchten. Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

   Einschränkungen bei der Benennung von Listen — Der Name Ihrer Liste kann Kleinbuchstaben, Großbuchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten.

2. Sie können dies auch tun, indem Sie den folgenden AWS Command Line Interface Befehl ausführen, `name` der die Liste aktualisiert und diese Liste auch aktiviert:

   ```
   aws guardduty update-trusted-entity-set \
   --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
   --name "AnyOrganization ListEXAMPLE" \
   --trusted-entity-set-id d4b94fc952d6912b8f3060768example \
   --activate
   ```

   `detector-id`Ersetzen Sie es durch die Melder-ID des Mitgliedskontos, für das Sie die Liste der vertrauenswürdigen Entitäten erstellen möchten, und durch andere Platzhalterwerte*shown in red*, die

   Wenn Sie diese neu erstellte Liste nicht aktivieren möchten, ersetzen Sie den Parameter `--activate` durch`--no-activate`.

   Der Parameter `expected-bucket-owner` ist optional. Unabhängig davon, ob Sie den Wert für diesen Parameter angeben oder nicht, wird GuardDuty überprüft, ob die mit diesem `--detector-id` Wert verknüpfte AWS-Konto ID den im `--location` Parameter angegebenen S3-Bucket besitzt. Wenn GuardDuty festgestellt wird, dass dieser S3-Bucket nicht zur angegebenen Konto-ID gehört, erhalten Sie bei der Aktivierung dieser Liste eine Fehlermeldung.

Gilt nur für benutzerdefinierte Bedrohungsgruppen und benutzerdefinierte Gruppen vertrauenswürdiger Entitäten — Wenn Sie eine Standort-URL angeben, die nicht den folgenden unterstützten Formaten entspricht, erhalten Sie beim Hinzufügen und Aktivieren der Liste eine Fehlermeldung.

Um eine Liste bedrohlicher Entitäten zu aktualisieren und zu aktivieren

1. Führen Sie UpdateThreatEntitySet. Stellen Sie sicher, dass Sie das `detectorId` Mitgliedskonto angeben, für das Sie diese Liste der Bedrohungsentitäten erstellen möchten. Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

   Einschränkungen bei der Benennung von Listen — Der Name Ihrer Liste kann Kleinbuchstaben, Großbuchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten.

2. Sie können dies auch tun, indem Sie den folgenden AWS Command Line Interface Befehl ausführen, `name` der die Liste aktualisiert und diese Liste auch aktiviert:

   ```
   aws guardduty update-threat-entity-set \
   --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
   --name "AnyOrganization ListEXAMPLE" \
   --threat-entity-set-id d4b94fc952d6912b8f3060768example \
   --activate
   ```

   `detector-id`Ersetzen Sie es durch die Melder-ID des Mitgliedskontos, für das Sie die Liste der Bedrohungsentitäten erstellen möchten, und durch andere Platzhalterwerte, die lauten*shown in red*.

   Wenn Sie diese neu erstellte Liste nicht aktivieren möchten, ersetzen Sie den Parameter `--activate` durch`--no-activate`.

   Der Parameter `expected-bucket-owner` ist optional. Unabhängig davon, ob Sie den Wert für diesen Parameter angeben oder nicht, wird GuardDuty überprüft, ob die mit diesem `--detector-id` Wert verknüpfte AWS-Konto ID den im `--location` Parameter angegebenen S3-Bucket besitzt. Wenn GuardDuty festgestellt wird, dass dieser S3-Bucket nicht zur angegebenen Konto-ID gehört, erhalten Sie bei der Aktivierung dieser Liste eine Fehlermeldung.

Gilt nur für benutzerdefinierte Bedrohungsgruppen und benutzerdefinierte Gruppen vertrauenswürdiger Entitäten — Wenn Sie eine Standort-URL angeben, die nicht den folgenden unterstützten Formaten entspricht, erhalten Sie beim Hinzufügen und Aktivieren der Liste eine Fehlermeldung.

Um eine Liste vertrauenswürdiger IP-Adressen zu aktualisieren und zu aktivieren

1. Führen Sie CreateIPSet aus. Stellen Sie sicher, dass Sie das Mitgliedskonto angeben, für das Sie diese Liste vertrauenswürdiger IP-Adressen aktualisieren möchten. `detectorId` Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

   Einschränkungen bei der Benennung von Listen — Der Name Ihrer Liste kann Kleinbuchstaben, Großbuchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten.

   Bei einer IP-Adressliste muss der Name Ihrer Liste innerhalb einer AWS-Konto UND-Region eindeutig sein.
2. Alternativ können Sie dies tun, indem Sie den folgenden AWS Command Line Interface Befehl ausführen, der auch die Liste aktiviert:

   ```
   aws guardduty update-ip-set \
   --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
   --name "AnyOrganization ListEXAMPLE" \
   --ip-set-id d4b94fc952d6912b8f3060768example \
   --activate
   ```

   `detector-id`Ersetzen Sie es durch die Melder-ID des Mitgliedskontos, für das Sie die Liste der vertrauenswürdigen IP-Adressen aktualisieren möchten, und durch andere Platzhalterwerte, die es sind*shown in red*.

   Wenn Sie diese neu erstellte Liste nicht aktivieren möchten, ersetzen Sie den Parameter `--activate` durch`--no-activate`.

   Der Parameter `expected-bucket-owner` ist optional. Wenn Sie die Konto-ID nicht angeben, der der S3-Bucket gehört, führt GuardDuty keine Überprüfung durch. Wenn Sie die Konto-ID für den `expected-bucket-owner` Parameter angeben, wird GuardDuty überprüft, ob diese AWS-Konto ID den im `--location` Parameter angegebenen S3-Bucket besitzt.

Wenn GuardDuty festgestellt wird, dass dieser S3-Bucket nicht zur angegebenen Konto-ID gehört, erhalten Sie bei der Aktivierung dieser Liste eine Fehlermeldung.

Um Bedrohungs-IP-Listen hinzuzufügen und zu aktivieren

1. Führen Sie CreateThreatIntelSet. Stellen Sie sicher, dass Sie das `detectorId` Mitgliedskonto angeben, für das Sie diese Bedrohungs-IP-Adressliste erstellen möchten. Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.

   Einschränkungen bei der Benennung von Listen — Der Name Ihrer Liste kann Kleinbuchstaben, Großbuchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten.

   Bei einer IP-Adressliste muss der Name Ihrer Liste innerhalb einer AWS-Konto UND-Region eindeutig sein.

2. Alternativ können Sie dies tun, indem Sie den folgenden AWS Command Line Interface Befehl ausführen, der auch die Liste aktiviert:

   ```
   aws guardduty update-threat-intel-set \
   --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
   --name "AnyOrganization ListEXAMPLE" \
   --threat-intel-set-id d4b94fc952d6912b8f3060768example \
   --activate
   ```

   `detector-id`Ersetzen Sie es durch die Melder-ID des Mitgliedskontos, für das Sie die Bedrohungs-IP-Liste aktualisieren möchten, und durch andere Platzhalterwerte, die es sind*shown in red*.

   Wenn Sie diese neu erstellte Liste nicht aktivieren möchten, ersetzen Sie den Parameter `--activate` durch`--no-activate`.

   Der Parameter `expected-bucket-owner` ist optional. Wenn Sie die Konto-ID nicht angeben, der der S3-Bucket gehört, führt GuardDuty keine Überprüfung durch. Wenn Sie die Konto-ID für den `expected-bucket-owner` Parameter angeben, wird GuardDuty überprüft, ob diese AWS-Konto ID den im `--location` Parameter angegebenen S3-Bucket besitzt. Wenn GuardDuty festgestellt wird, dass dieser S3-Bucket nicht zur angegebenen Konto-ID gehört, erhalten Sie bei der Aktivierung dieser Liste eine Fehlermeldung.

De-activating Entitätsliste oder IP-Adressliste

Wenn Sie eine Liste nicht mehr verwenden GuardDuty möchten, können Sie sie deaktivieren. Es kann einige Minuten dauern, bis der Vorgang abgeschlossen ist. Weitere Informationen finden Sie unter Wichtige Überlegungen zu GuardDuty Listen. Nach der Deaktivierung der Liste wirken sich die Einträge in der Entitäts- oder IP-Adressliste nicht mehr auf die Bedrohungserkennung in GuardDuty aus.

Wählen Sie eine der Zugriffsmethoden, um die Liste zu deaktivieren.

Console

Um die Entitätsliste oder die IP-Adressliste zu deaktivieren

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Listen.
3. Wählen Sie auf der Listenseite die Registerkarte aus, auf der Sie die Liste deaktivieren möchten — Entitätslisten oder IP-Adressliste.
4. Wählen Sie auf der ausgewählten Registerkarte die Liste aus, die Sie deaktivieren möchten.
5. Wählen Sie Aktionen und dann Deaktivieren aus.
6. Bestätigen Sie die Aktion und wählen Sie Deaktivieren.

API/CLI

Um mit den folgenden Verfahren zu beginnen, benötigen Sie die ID, z. B.`trustedEntitySetId`, `threatEntitySetIdtrustedIpSet`, oder`threatIpSet`, die der Listenressource zugeordnet ist, die Sie deaktivieren möchten.

Um eine Liste vertrauenswürdiger Entitäten zu deaktivieren

1. Führen Sie UpdateTrustedEntitySet. Stellen Sie sicher, dass Sie das `detectorId` Mitgliedskonto angeben, für das Sie diese Liste vertrauenswürdiger Entitäten deaktivieren möchten. Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.
2. Sie können dies auch tun, indem Sie den folgenden AWS Command Line Interface Befehl ausführen:

```
aws guardduty update-trusted-entity-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--trusted-entity-set-id d4b94fc952d6912b8f3060768example \
--no-activate
```

`detector-id`Ersetzen Sie es durch die Melder-ID des Mitgliedskontos, für das Sie die Liste der vertrauenswürdigen Entitäten deaktivieren möchten, und durch andere Platzhalterwerte, die es sind*shown in red*.

Um Listen mit Bedrohungsentitäten zu deaktivieren

1. Führen Sie UpdateThreatEntitySet. Stellen Sie sicher, dass Sie das `detectorId` Mitgliedskonto angeben, für das Sie diese Liste der Bedrohungsentitäten deaktivieren möchten. Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.
2. Sie können dies auch tun, indem Sie den folgenden AWS Command Line Interface Befehl ausführen:

```
aws guardduty update-threat-entity-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--threat-entity-set-id d4b94fc952d6912b8f3060768example \
--no-activate
```

`detector-id`Ersetzen Sie es durch die Melder-ID des Mitgliedskontos, für das Sie die Liste der Bedrohungsentitäten erstellen, und durch andere Platzhalterwerte*shown in red*, die

Um eine Liste vertrauenswürdiger IP-Adressen zu deaktivieren

1. Führen Sie UpdateIPSet aus. Stellen Sie sicher, dass Sie das `detectorId` Mitgliedskonto angeben, für das Sie diese Liste vertrauenswürdiger IP-Adressen deaktivieren möchten. Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.
2. Sie können dies auch tun, indem Sie den folgenden AWS Command Line Interface Befehl ausführen und sicherstellen, dass Sie das durch die `detector-id` Melder-ID

des Mitgliedskontos ersetzen, für das Sie die Liste der vertrauenswürdigen IP-Adressen deaktivieren möchten.

```
aws guardduty update-ip-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--ip-set-id d4b94fc952d6912b8f3060768example \
--no-activate
```

Um die Bedrohungs-IP-Liste zu deaktivieren

1. Führen Sie UpdateThreatIntelSet. Stellen Sie sicher, dass Sie das `detectorId` Mitgliedskonto angeben, für das Sie diese Bedrohungs-IP-Adressliste deaktivieren möchten. Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.
2. Sie können dies auch tun, indem Sie den folgenden AWS Command Line Interface Befehl ausführen und sicherstellen, dass Sie das durch die `detector-id` Melder-ID des Mitgliedskontos ersetzen, für das Sie die Bedrohungs-IP-Liste deaktivieren möchten.

```
aws guardduty update-threat-intel-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--threat-intel-set-id d4b94fc952d6912b8f3060768example \
--no-activate
```

Entitätsliste oder IP-Adressliste löschen

Wenn Sie einen Listeneintrag in Ihrem Entitätsatz oder IP-Adresssatz nicht mehr behalten möchten, können Sie ihn löschen. Es kann einige Minuten dauern, bis der Vorgang abgeschlossen ist. Weitere Informationen finden Sie unter Wichtige Überlegungen zu GuardDuty Listen.

Wenn der Status der Liste Aktiviert oder Deaktiviert lautet, müssen Sie einige Minuten warten, bevor Sie eine Aktion ausführen. Weitere Informationen finden Sie unter Grundlegendes zum Listenstatus.

Wählen Sie eine der Zugriffsmethoden, um die Liste zu löschen.

Console

Um die Entitätsliste oder die IP-Adressliste zu löschen

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Listen.
3. Wählen Sie auf der Listenseite die Registerkarte aus, in der Sie die Liste löschen möchten — Entitätslisten oder IP-Adressliste.
4. Wählen Sie auf der ausgewählten Registerkarte die Liste aus, die Sie löschen möchten.
5. Wählen Sie Aktionen und anschließend Löschen aus.

   Der Status der Liste ändert sich in „Ausstehend löschen“. Es kann einige Minuten dauern, bis die Liste gelöscht wird.

API/CLI

Um mit den folgenden Verfahren zu beginnen, benötigen Sie die ID, z. B.`trustedEntitySetId`, `threatEntitySetIdtrustedIpSet`, oder`threatIpSet`, die der Listenressource zugeordnet ist, die Sie löschen möchten.

Um eine Liste vertrauenswürdiger Entitäten zu löschen

1. Führen Sie DeleteTrustedEntitySet. Stellen Sie sicher, dass Sie das `detectorId` Mitgliedskonto angeben, für das Sie diese Liste der vertrauenswürdigen Entitäten löschen möchten. Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.
2. Sie können dies auch tun, indem Sie den folgenden AWS Command Line Interface Befehl ausführen:

   ```
   aws guardduty delete-trusted-entity-set \
   --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
   --trusted-entity-set-id d4b94fc952d6912b8f3060768example
   ```

   `detector-id`Ersetzen Sie es durch die Melder-ID des Mitgliedskontos, für das Sie die Liste der vertrauenswürdigen Entitäten löschen möchten, und durch andere Platzhalterwerte, die vorhanden sind*shown in red*.

Um Listen mit Bedrohungsentitäten zu deaktivieren

1. Führen Sie DeleteThreatEntitySet. Stellen Sie sicher, dass Sie das `detectorId` Mitgliedskonto angeben, für das Sie diese Liste der Bedrohungsentitäten löschen möchten. Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.
2. Sie können dies auch tun, indem Sie den folgenden AWS Command Line Interface Befehl ausführen:

```
aws guardduty delete-threat-entity-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--threat-entity-set-id d4b94fc952d6912b8f3060768example
```

`detector-id`Ersetzen Sie es durch die Melder-ID des Mitgliedskontos, für das Sie die Liste der Bedrohungsentitäten löschen möchten, und durch andere Platzhalterwerte, die vorhanden sind*shown in red*.

Um eine Liste vertrauenswürdiger IP-Adressen zu löschen

1. Führen Sie DeleteIPSet aus. Stellen Sie sicher, dass Sie das `detectorId` Mitgliedskonto angeben, für das Sie diese Liste vertrauenswürdiger IP-Adressen löschen möchten. Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.
2. Sie können dies auch tun, indem Sie den folgenden AWS Command Line Interface Befehl ausführen und sicherstellen, dass Sie das durch die `detector-id` Melder-ID des Mitgliedskontos ersetzen, für das Sie die Liste der vertrauenswürdigen IP-Adressen löschen möchten.

```
aws guardduty delete-ip-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--ip-set-id d4b94fc952d6912b8f3060768example
```

`detector-id`Ersetzen Sie es durch die Melder-ID des Mitgliedskontos, für das Sie die Liste der Bedrohungsentitäten löschen möchten, und durch andere Platzhalterwerte, die es sind*shown in red*.

Um die Liste der Bedrohungs-IP-Adressen zu löschen

1. Führen Sie DeleteThreatIntelSet. Stellen Sie sicher, dass Sie das `detectorId` Mitgliedskonto angeben, für das Sie diese Bedrohungs-IP-Adressliste löschen möchten. Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie die ListDetectorsAPI aus.
2. Sie können dies auch tun, indem Sie den folgenden AWS Command Line Interface Befehl ausführen und sicherstellen, dass Sie das durch die `detector-id` Melder-ID des Mitgliedskontos ersetzen, für das Sie die Bedrohungs-IP-Liste löschen möchten.

   ```
   aws guardduty delete-threat-intel-set \
   --detector-id 12abc34d567e8fa901bc2d34e56789f0 \
   --threat-intel-set-id d4b94fc952d6912b8f3060768example
   ```

   `detector-id`Ersetzen Sie es durch die Melder-ID des Mitgliedskontos, für das Sie die Liste der Bedrohungsentitäten löschen möchten, und durch andere Platzhalterwerte, die es sind*shown in red*.

Generierte GuardDuty Ergebnisse in Amazon S3-Buckets exportieren

GuardDuty speichert die generierten Ergebnisse für einen Zeitraum von 90 Tagen. GuardDuty exportiert die aktiven Ergebnisse nach Amazon EventBridge (EventBridge). Sie können die generierten Ergebnisse optional in einen Amazon Simple Storage Service (Amazon S3) -Bucket exportieren. Auf diese Weise können Sie die historischen Daten potenziell verdächtiger Aktivitäten in Ihrem Konto nachverfolgen und beurteilen, ob die empfohlenen Abhilfemaßnahmen erfolgreich waren.

Alle neuen aktiven Ergebnisse, die GuardDuty generiert werden, werden innerhalb von etwa 5 Minuten nach der Generierung des Ergebnisses automatisch exportiert. Sie können die Häufigkeit festlegen, in der Aktualisierungen der aktiven Ergebnisse exportiert werden EventBridge. Die von Ihnen gewählte Häufigkeit gilt für den Export neuer Vorkommen vorhandener Ergebnisse in Ihren S3-Bucket (sofern konfiguriert) und Detective (wenn integriert). EventBridge Informationen darüber, wie mehrere Vorkommen vorhandener Ergebnisse GuardDuty aggregiert werden, finden Sie unter. GuardDuty Aggregation finden

Wenn Sie Einstellungen für den Export von Ergebnissen in einen Amazon S3-Bucket konfigurieren, GuardDuty verwendet AWS Key Management Service (AWS KMS), um die Ergebnisdaten in Ihrem S3-Bucket zu verschlüsseln. Dazu müssen Sie Ihrem S3-Bucket und dem AWS KMS Schlüssel Berechtigungen hinzufügen, damit Sie diese zum Exportieren der Ergebnisse in Ihrem Konto verwenden GuardDuty können.

Inhalt

- Überlegungen
- Schritt 1 — Zum Exportieren der Ergebnisse sind Berechtigungen erforderlich
- Schritt 2 — Richtlinie an Ihren KMS-Schlüssel anhängen
- Schritt 3 — Richtlinie an den Amazon S3-Bucket anhängen
- Schritt 4 — Ergebnisse in einen S3-Bucket exportieren (Konsole)
- Schritt 5 — Häufigkeit für den Export aktualisierter aktiver Ergebnisse festlegen

Überlegungen

Bevor Sie mit den Voraussetzungen und Schritten für den Export von Ergebnissen fortfahren, sollten Sie die folgenden Schlüsselkonzepte berücksichtigen:

- Die Exporteinstellungen sind regional — Sie müssen die Exportoptionen in jeder Region konfigurieren, die Sie verwenden GuardDuty.
- Ergebnisse in Amazon S3-Buckets in verschiedenen AWS-Regionen (regionsübergreifenden) Bereichen exportieren — GuardDuty unterstützt die folgenden Exporteinstellungen:
  - Ihr Amazon S3-Bucket oder -Objekt und der AWS KMS Schlüssel müssen zu demselben gehören. AWS-Region
  - Für die Ergebnisse, die in einer kommerziellen Region generiert wurden, können Sie diese Ergebnisse in einen S3-Bucket in einer beliebigen kommerziellen Region exportieren. Sie können diese Ergebnisse jedoch nicht in einen S3-Bucket in einer Opt-in-Region exportieren.
  - Für die Ergebnisse, die in einer Opt-in-Region generiert wurden, können Sie wählen, ob Sie diese Ergebnisse in dieselbe Opt-in-Region exportieren möchten, in der sie generiert wurden, oder in eine beliebige kommerzielle Region. Sie können jedoch keine Ergebnisse aus einer Opt-in-Region in eine andere Opt-in-Region exportieren.
- Berechtigungen zum Exportieren von Ergebnissen — Um Einstellungen für den Export aktiver Ergebnisse zu konfigurieren, muss Ihr S3-Bucket über Berechtigungen verfügen, die das

Hochladen von GuardDuty Objekten ermöglichen. Sie benötigen außerdem einen AWS KMS Schlüssel, mit dem Sie Ergebnisse verschlüsseln GuardDuty können.

- Archivierte Ergebnisse werden nicht exportiert — Das Standardverhalten ist, dass die archivierten Ergebnisse, einschließlich neuer Instanzen unterdrückter Ergebnisse, nicht exportiert werden.

  Wenn ein GuardDuty Ergebnis als Archiviert generiert wird, müssen Sie die Archivierung aufheben. Dadurch wird der Suchstatus des Filters in Aktiv geändert. GuardDuty exportiert die Aktualisierungen je nach Konfiguration Schritt 5 — Häufigkeit für den Export von Ergebnissen in die vorhandenen, nicht archivierten Ergebnisse.

- GuardDuty Administratorkonto kann Ergebnisse exportieren, die in verknüpften Mitgliedskonten generiert wurden — Wenn Sie Exportergebnisse in einem Administratorkonto konfigurieren, werden alle Ergebnisse der zugehörigen Mitgliedskonten, die in derselben Region generiert wurden, ebenfalls an den Speicherort exportiert, den Sie für das Administratorkonto konfiguriert haben. Weitere Informationen finden Sie unter Grundlegendes zur Beziehung zwischen GuardDuty Administratorkonto und Mitgliedskonten.

Schritt 1 — Zum Exportieren der Ergebnisse sind Berechtigungen erforderlich

Wenn Sie Einstellungen für den Export von Ergebnissen konfigurieren, wählen Sie einen Amazon S3-Bucket aus, in dem Sie die Ergebnisse und einen AWS KMS Schlüssel für die Datenverschlüsselung speichern können. Zusätzlich zu den Berechtigungen für GuardDuty Aktionen müssen Sie auch über Berechtigungen für die folgenden Aktionen verfügen, um die Einstellungen für den Export von Ergebnissen erfolgreich zu konfigurieren:

- `s3:GetBucketLocation`
- `s3:PutObject`

Wenn Sie die Ergebnisse an ein bestimmtes Präfix in Ihrem Amazon S3-Bucket exportieren müssen, müssen Sie der IAM-Rolle außerdem die folgenden Berechtigungen hinzufügen:

- `s3:GetObject`
- `s3:ListBucket`

Schritt 2 — Richtlinie an Ihren KMS-Schlüssel anhängen

GuardDuty verschlüsselt die Ergebnisdaten in Ihrem Bucket mithilfe von. AWS Key Management Service Um die Einstellungen erfolgreich zu konfigurieren, müssen Sie zunächst die GuardDuty Erlaubnis zur Verwendung eines KMS-Schlüssels erteilen. Sie können die Berechtigungen gewähren, indem Sie die Richtlinie an Ihren KMS-Schlüssel anhängen.

Wenn Sie einen KMS-Schlüssel von einem anderen Konto verwenden, müssen Sie die Schlüsselrichtlinie anwenden, indem Sie sich bei dem Konto anmelden AWS-Konto , das den Schlüssel besitzt. Wenn Sie die Einstellungen für den Export von Ergebnissen konfigurieren, benötigen Sie auch den Schlüssel-ARN des Kontos, dem der Schlüssel gehört.

Um die KMS-Schlüsselrichtlinie für die Verschlüsselung Ihrer exportierten Ergebnisse GuardDuty zu ändern

1. Öffnen Sie die AWS KMS Konsole unter. https://console.aws.amazon.com/kms
2. Um das zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
3. Wählen Sie einen vorhandenen KMS-Schlüssel aus, oder führen Sie im AWS Key Management Service Entwicklerhandbuch die Schritte zum Erstellen eines neuen Schlüssels aus, den Sie zum Verschlüsseln der exportierten Ergebnisse verwenden werden.

   > **Note**
   >
   > Der AWS-Region Ihres KMS-Schlüssels und des Amazon S3-Buckets müssen identisch sein.

   Sie können dasselbe S3-Bucket- und KMS-Schlüsselpaar verwenden, um die Ergebnisse aus einer beliebigen Region zu exportieren. Weitere Informationen finden Sie unter Informationen Überlegungen zum regionsübergreifenden Exportieren von Ergebnissen.
4. Wählen Sie im Abschnitt Key policy (Schlüsselrichtlinie) die Option Edit (Bearbeiten) aus.

   Wenn Zur Richtlinienansicht wechseln angezeigt wird, wählen Sie diese Ansicht aus, um die Schlüsselrichtlinie anzuzeigen, und klicken Sie dann auf Bearbeiten.
5. Kopieren Sie den folgenden Richtlinienblock in Ihre KMS-Schlüsselrichtlinie, um die GuardDuty Erlaubnis zur Verwendung Ihres Schlüssels zu erteilen.

```
{
    "Sid": "AllowGuardDutyKey",
    "Effect": "Allow",
    "Principal": {
        "Service": "guardduty.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey",
    "Resource": "KMS key ARN",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "123456789012",
            "aws:SourceArn":
 "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
        }
    }
}
```

6. Bearbeiten Sie die Richtlinie, indem Sie die folgenden Werte ersetzen, die *red* im Richtlinienbeispiel formatiert sind:

   1. *KMS key ARN*Ersetzen Sie den KMS-Schlüssel durch den Amazon-Ressourcennamen (ARN). Informationen zum Auffinden des Schlüssel-ARN finden Sie unter Suchen der Schlüssel-ID und des ARN im AWS Key Management Service Entwicklerhandbuch.
   2. *123456789012*Ersetzen Sie es durch die AWS-Konto ID, der das GuardDuty Konto gehört, das die Ergebnisse exportiert.
   3. *Region2*Ersetzen Sie durch den AWS-Region Ort, an dem die GuardDuty Ergebnisse generiert werden.
   4. *SourceDetectorID*Ersetzen Sie es durch das GuardDuty Konto in der spezifischen Region, in der die Ergebnisse generiert wurden. `detectorID`

      Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`

> **Note**
>
> Wenn Sie es GuardDuty in einer Opt-in-Region verwenden, ersetzen Sie den Wert für den „Dienst“ durch den regionalen Endpunkt für diese Region. Wenn Sie beispielsweise

GuardDuty in der Region Naher Osten (Bahrain) (me-south-1) verwenden, ersetzen Sie es durch. `"Service": "guardduty.amazonaws.com"` `"Service": "guardduty.me-south-1.amazonaws.com"` Informationen zu Endpunkten für jede Opt-in-Region finden Sie unter GuardDuty Endpunkte und Kontingente.

7. Wenn Sie die Grundsatzerklärung vor der endgültigen Aussage hinzugefügt haben, fügen Sie ein Komma hinzu, bevor Sie diese Aussage hinzufügen. Stellen Sie sicher, dass die JSON-Syntax Ihrer KMS-Schlüsselrichtlinie gültig ist.

   Wählen Sie Speichern.

8. (Optional) Kopieren Sie den Schlüssel-ARN in einen Notizblock, um ihn in den späteren Schritten zu verwenden.

Schritt 3 — Richtlinie an den Amazon S3-Bucket anhängen

Fügen Sie dem Amazon S3-Bucket, in den Sie Ergebnisse exportieren, Berechtigungen hinzu, damit Objekte in diesen S3-Bucket hochgeladen werden GuardDuty können. Unabhängig davon, ob Sie einen Amazon S3-Bucket verwenden, der entweder zu Ihrem Konto oder zu einem anderen Konto gehört AWS-Konto, müssen Sie diese Berechtigungen hinzufügen.

Wenn Sie sich zu einem beliebigen Zeitpunkt dazu entschließen, Ergebnisse in einen anderen S3-Bucket zu exportieren, müssen Sie diesem S3-Bucket Berechtigungen hinzufügen und die Einstellungen für den Export der Ergebnisse erneut konfigurieren, um den Export der Ergebnisse fortzusetzen.

Wenn Sie noch keinen Amazon S3-Bucket haben, in den Sie diese Ergebnisse exportieren möchten, finden Sie weitere Informationen unter Erstellen eines Buckets im Amazon S3-Benutzerhandbuch.

Um Ihrer S3-Bucket-Richtlinie Berechtigungen zuzuweisen

1. Führen Sie die Schritte unter So erstellen oder bearbeiten Sie eine Bucket-Richtlinie im Amazon S3-Benutzerhandbuch aus, bis die Seite Bucket-Richtlinie bearbeiten angezeigt wird.
2. Die Beispielrichtlinie zeigt, wie Sie die GuardDuty Erlaubnis zum Exportieren von Ergebnissen in Ihren Amazon S3-Bucket erteilen. Wenn Sie den Pfad ändern, nachdem Sie die Exportergebnisse konfiguriert haben, müssen Sie die Richtlinie ändern, um die Genehmigung für den neuen Standort zu erteilen.

Kopieren Sie die folgende Beispielrichtlinie und fügen Sie sie in den Bucket-Richtlinien-Editor ein.

Wenn Sie die Richtlinienanweisung vor der endgültigen Aussage hinzugefügt haben, fügen Sie vor dem Hinzufügen dieser Anweisung ein Komma hinzu. Stellen Sie sicher, dass die JSON-Syntax Ihrer KMS-Schlüsselrichtlinie gültig ist.

Beispiel für eine S3-Bucket-Richtlinie

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Allow GetBucketLocation",
            "Effect": "Allow",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:GetBucketLocation",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "aws:SourceArn": "arn:aws:guardduty:us-
east-2:123456789012:detector/SourceDetectorID"

                }
            }
        },
        {
            "Sid": "Allow PutObject",
            "Effect": "Allow",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional prefix]/
*",
            "Condition": {
```

```
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "aws:SourceArn": "arn:aws:guardduty:us-
east-2:123456789012:detector/SourceDetectorID"

                }
            }
        },
        {
            "Sid": "Deny unencrypted object uploads",
            "Effect": "Deny",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional prefix]/
*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption": "aws:kms"
                }
            }
        },
        {
            "Sid": "Deny incorrect encryption header",
            "Effect": "Deny",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional prefix]/
*",
            "Condition": {
                "StringNotEquals": {
                "s3:x-amz-server-side-encryption-aws-kms-key-id":
 "arn:aws:kms:us-east-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
                }
            }
        },
        {
            "Sid": "Deny non-HTTPS access",
            "Effect": "Deny",
            "Principal": "*",
```

```
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional prefix]/
*",
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

3. Bearbeiten Sie die Richtlinie, indem Sie die folgenden Werte ersetzen, die *red* im Richtlinienbeispiel formatiert sind:

   1. *Amazon S3 bucket ARN*Ersetzen Sie ihn durch den Amazon-Ressourcennamen (ARN) des Amazon S3-Buckets. Sie finden den Bucket-ARN auf der Seite „Bucket-Richtlinie bearbeiten“ in der https://console.aws.amazon.com/s3/ Konsole.
   2. *123456789012*Ersetzen Sie ihn durch die AWS-Konto ID, der das GuardDuty Konto gehört, das die Ergebnisse exportiert.
   3. *us-east-2*Ersetzen Sie durch den AWS-Region Ort, an dem die GuardDuty Ergebnisse generiert werden.
   4. *SourceDetectorID*Ersetzen Sie es durch das GuardDuty Konto in der spezifischen Region, in der die Ergebnisse generiert wurden. `detectorID`

      Informationen zu Ihrem Konto und Ihrer aktuellen Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ Konsole oder führen Sie die ListDetectors API aus. `detectorId`
   5. Ersetzen Sie einen *[optional prefix]* Teil des *S3 bucket ARN/[optional prefix]* Platzhalterwerts durch einen optionalen Speicherort des Ordners, in den Sie die Ergebnisse exportieren möchten. Weitere Informationen zur Verwendung von Präfixen finden Sie unter Organisieren von Objekten mithilfe von Präfixen im Amazon S3-Benutzerhandbuch.

      Wenn Sie einen optionalen Ordnerspeicherort angeben, muss der Ordner bereits im S3-Bucket vorhanden sein. GuardDuty erstellt den Ordner nicht in Ihrem Namen. Diese Anforderung gilt unabhängig davon, ob der Bucket Eigentümer ist.
   6. Ersetzen Sie den KMS-Schlüssel, der *KMS key ARN* mit der Verschlüsselung der in den S3-Bucket exportierten Ergebnisse verknüpft ist, durch den Amazon-Ressourcennamen (ARN).

Informationen zum Auffinden des Schlüssel-ARN finden Sie unter Suchen der Schlüssel-ID und des ARN im AWS Key Management Service Entwicklerhandbuch.

> **Note**
>
> Wenn Sie es GuardDuty in einer Opt-in-Region verwenden, ersetzen Sie den Wert für den „Service“ durch den regionalen Endpunkt für diese Region. Wenn Sie beispielsweise GuardDuty in der Region Naher Osten (Bahrain) (me-south-1) verwenden, ersetzen Sie es durch. `"Service": "guardduty.amazonaws.com"` `"Service": "guardduty.me-south-1.amazonaws.com"` Informationen zu Endpunkten für jede Opt-in-Region finden Sie unter GuardDuty Endpunkte und Kontingente.

4. Wählen Sie Speichern.

Schritt 4 — Ergebnisse in einen S3-Bucket exportieren (Konsole)

GuardDuty ermöglicht es Ihnen, Ergebnisse in einen vorhandenen Bucket in einem anderen zu exportieren AWS-Konto.

Wenn Sie einen neuen S3-Bucket erstellen oder einen vorhandenen Bucket in Ihrem Konto auswählen, können Sie ein optionales Präfix hinzufügen. Sowohl das Präfix als auch der Ordnerpfad, in den die Ergebnisse geschrieben werden, müssen bereits im S3-Bucket vorhanden sein. GuardDuty erstellt keine Ordner in Ihrem Namen. GuardDuty schreibt Ergebnisobjekte in den Pfad/`AWSLogs/`*`123456789012`*`/GuardDuty/`*`Region`*, daher müssen Sie diese Ordnerstruktur erstellen, bevor Sie Ergebnisse exportieren.

Der gesamte Pfad des S3-Objekts wird sein*`amzn-s3-demo-bucket`*`/`*`prefix-name`*`/` `UUID`*`.jsonl.gz`*. Der `UUID` wird nach dem Zufallsprinzip generiert und stellt weder die Detektor-ID noch die Befund-ID dar.

> **Important**
>
> Der KMS-Schlüssel und der S3-Bucket müssen sich in derselben Region befinden.

Bevor Sie diese Schritte ausführen, stellen Sie sicher, dass Sie die entsprechenden Richtlinien an Ihren KMS-Schlüssel und den vorhandenen S3-Bucket angehängt haben.

So konfigurieren Sie die Exportergebnisse

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie auf der Seite Einstellungen unter Exportoptionen für Ergebnisse für S3-Bucket die Option Jetzt konfigurieren (oder je nach Bedarf Bearbeiten) aus.
4. Geben Sie für S3-Bucket-ARN den ein**`bucket ARN`**. Informationen zum Bucket-ARN finden Sie unter Anzeigen der Eigenschaften für einen S3-Bucket im Amazon S3-Benutzerhandbuch.
5. Geben Sie für den KMS-Schlüssel-ARN den ein **`key ARN`**. Informationen zum Auffinden des Schlüssel-ARN finden Sie unter Suchen der Schlüssel-ID und des ARN im AWS Key Management Service Entwicklerhandbuch.
6. Richtlinien anhängen

   - Führen Sie die Schritte aus, um die S3-Bucket-Richtlinie anzuhängen. Weitere Informationen finden Sie unter Schritt 3 — Richtlinie an den Amazon S3-Bucket anhängen.

   - Führen Sie die Schritte aus, um die KMS-Schlüsselrichtlinie anzuhängen. Weitere Informationen finden Sie unter Schritt 2 — Richtlinie an Ihren KMS-Schlüssel anhängen.
7. Wählen Sie Save (Speichern) aus.

Schritt 5 — Häufigkeit für den Export aktualisierter aktiver Ergebnisse festlegen

Konfigurieren Sie die Häufigkeit für den Export aktualisierter aktiver Ergebnisse entsprechend Ihrer Umgebung. Standardmäßig werden aktualisierte Ergebnisse alle 6 Stunden exportiert. Dies bedeutet, dass alle Ergebnisse in den nächsten Export aufgenommen werden, die nach dem letzten Export aktualisiert wurden. Wenn aktualisierte Ergebnisse alle 6 Stunden exportiert werden und dieser Export um 12:00 Uhr erfolgt, wird jedes nach 12:00 Uhr aktualisierte Ergebnis um 18:00 Uhr exportiert.

So stellen Sie die Häufigkeit ein

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie Einstellungen aus.

3. Wählen Sie im Bereich Exportoptionen für Erkenntnisse die Option Häufigkeit für aktualisierte Erkenntnisse aus. Dies legt die Häufigkeit fest, mit der aktualisierte Active-Ergebnisse EventBridge sowohl nach Amazon S3 als auch nach Amazon S3 exportiert werden. Sie können aus den folgenden Optionen auswählen:

   - Aktualisieren Sie S3 EventBridge und S3 alle 15 Minuten
   - Update EventBridge und S3 alle 1 Stunde
   - Update EventBridge und S3 alle 6 Stunden (Standard)
4. Wählen Sie Änderungen speichern aus.

Bearbeitung von GuardDuty Ergebnissen mit Amazon EventBridge

GuardDuty veröffentlicht (sendet) Ergebnisse automatisch als Ereignisse an Amazon EventBridge (ehemals Amazon CloudWatch Events), einen serverlosen Eventbus-Service. EventBridge liefert einen Stream von Daten aus Anwendungen und Services nahezu in Echtzeit an Ziele wie Amazon Simple Notification Service (Amazon SNS) -Themen, AWS Lambda -Funktionen und Amazon Kinesis Kinesis-Streams. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.

EventBridge ermöglicht die automatische Überwachung und Verarbeitung von GuardDuty Ergebnissen durch den Empfang von Ereignissen. EventBridge empfängt Ereignisse sowohl für neu generierte Ergebnisse als auch für aggregierte Ergebnisse, wobei nachfolgende Ereignisse eines vorhandenen Ergebnisses mit dem ursprünglichen Ergebnis kombiniert werden. Jedem GuardDuty Befund wird eine Befund-ID zugewiesen, und für jeden Befund GuardDuty wird ein EventBridge Ereignis mit einer eindeutigen Befund-ID erstellt. Informationen zur Funktionsweise der Aggregation in finden Sie GuardDuty unterGuardDuty Aggregation finden.

Zusätzlich zur automatisierten Überwachung und Verarbeitung EventBridge ermöglicht die Verwendung von eine längerfristige Aufbewahrung Ihrer Ergebnisdaten. GuardDuty speichert Ergebnisse für 90 Tage. Mit EventBridge können Sie Ergebnisdaten an Ihre bevorzugte Speicherplattform senden und die Daten so lange speichern, wie Sie möchten. Um Ergebnisse für einen längeren Zeitraum aufzubewahren, GuardDuty unterstütztGenerierte Ergebnisse nach Amazon S3 exportieren.

Themen

- Grundlegendes zur Häufigkeit von EventBridge Benachrichtigungen in GuardDuty
- Richten Sie ein Amazon SNS SNS-Thema und einen Endpunkt ein (E-Mail, Slack und Amazon Chime)

- Amazon EventBridge für GuardDuty Ergebnisse verwenden
- Eine EventBridge Regel für GuardDuty Ergebnisse erstellen
- EventBridge Regel für Umgebungen mit GuardDuty mehreren Konten

Grundlegendes zur Häufigkeit von EventBridge Benachrichtigungen in GuardDuty

In diesem Abschnitt wird erklärt, wie oft Sie Benachrichtigungen über Fundfälle erhalten EventBridge und wie Sie die Häufigkeit für nachfolgende Fundfälle aktualisieren können.

Benachrichtigungen für neu generierte Ergebnisse mit einer eindeutigen Befund-ID

GuardDuty sendet diese Benachrichtigungen nahezu in Echtzeit, wenn ein Ergebnis mit einer eindeutigen Befund-ID generiert wird. Die Benachrichtigung umfasst alle weiteren Vorkommen dieser Ergebnis-ID während der Generierung der Benachrichtigung.

Die Benachrichtigungshäufigkeit für neu generierte Ergebnisse erfolgt nahezu in Echtzeit. Standardmäßig können Sie diese Häufigkeit nicht ändern.

Benachrichtigungen für nachfolgende Erkenntnisse

GuardDuty fasst alle nachfolgenden Ereignisse eines bestimmten Ergebnistyps, die innerhalb der 6-Stunden-Intervalle stattfinden, zu einem einzigen Ereignis zusammen. Nur ein Administratorkonto kann die EventBridge Benachrichtigungshäufigkeit für nachfolgende Befunde aktualisieren. Ein Mitgliedskonto kann diese Häufigkeit nicht für sein eigenes Konto aktualisieren. Wenn das delegierte GuardDuty Administratorkonto die Häufigkeit beispielsweise auf eine Stunde aktualisiert, erhalten alle Mitgliedskonten außerdem eine einstündige Benachrichtigungsfrequenz über die nachfolgenden Ereignisse, die an gesendet werden. EventBridge Weitere Informationen finden Sie unter Mehrere Konten bei Amazon GuardDuty.

Als Administratorkonto können Sie die Standardhäufigkeit von Benachrichtigungen über nachfolgende Befunde anpassen. Mögliche Werte sind 15 Minuten, 1 Stunde oder standardmäßig 6 Stunden. Weitere Informationen zum Einrichten der Häufigkeit für diese Benachrichtigungen finden Sie unter Schritt 5 — Häufigkeit für den Export aktualisierter aktiver Ergebnisse festlegen.

Weitere Informationen darüber, wie das Administratorkonto EventBridge Benachrichtigungen für Mitgliedskonten erhält, finden Sie unterEventBridge Regel für Umgebungen mit mehreren Konten.

Richten Sie ein Amazon SNS SNS-Thema und einen Endpunkt ein (E-Mail, Slack und Amazon Chime)

Amazon Simple Notification Service (Amazon SNS) ist ein vollständig verwalteter Service, der die Nachrichtenzustellung von Verlagen an Abonnenten ermöglicht. Herausgeber kommunizieren asynchron mit Abonnenten, indem sie Nachrichten zu einem Thema senden. Ein Thema ist ein logischer Zugriffspunkt und Kommunikationskanal, mit dem Sie mehrere Endpunkte wie AWS Lambda Amazon Simple Queue Service (Amazon SQS) und eine E-Mail-Adresse gruppieren können. HTTP/S

> **Note**
>
> Sie können Ihrer bevorzugten EventBridge Ereignisregel während oder nach der Erstellung der Regel ein Amazon SNS SNS-Thema hinzufügen.

Erstellen Sie ein Amazon SNS SNS-Thema

Zu Beginn müssen Sie zunächst ein Thema in Amazon SNS einrichten und einen Endpunkt hinzufügen. Um ein Thema zu erstellen, führen Sie die Schritte in Schritt 1: Thema erstellen im Amazon Simple Notification Service Developer Guide aus. Nachdem das Thema erstellt wurde, kopieren Sie den Themen-ARN in die Zwischenablage. Sie werden dieses Thema ARN verwenden, um mit einem der bevorzugten Setups fortzufahren.

Wählen Sie eine bevorzugte Methode, um festzulegen, wohin Sie die Suchdaten senden GuardDuty möchten.

Email setup

Um einen E-Mail-Endpunkt einzurichten

Nach Ihnen Create an Amazon SNS topic besteht der nächste Schritt darin, ein Abonnement für dieses Thema zu erstellen. Führen Sie die Schritte unter Schritt 2: Erstellen eines Abonnements für ein Amazon SNS SNS-Thema im Amazon Simple Notification Service Developer Guide durch.

1. Verwenden Sie für Themen-ARN den Themen-ARN, den Sie in diesem Create an Amazon SNS topic Schritt erstellt haben. Das Thema ARN sieht in etwa wie folgt aus:

```
arn:aws:sns:us-east-2:123456789012:your_topic
```

2. Wählen Sie unter Protocol die Option Email aus.
3. Geben Sie für Endpoint eine E-Mail-Adresse ein, unter der Sie die Benachrichtigungen von Amazon SNS erhalten möchten.

   Nachdem das Abonnement erstellt wurde, müssen Sie es über Ihren E-Mail-Client bestätigen.

Slack setup

So konfigurierst du einen Amazon Q Developer in einem Client für Chat-Anwendungen - Slack

Danach besteht der nächste Schritt darinCreate an Amazon SNS topic, den Client für Slack zu konfigurieren.

Führe die Schritte unter Tutorial: Erste Schritte mit Slack im Administratorhandbuch für Amazon Q Developer in Chat-Anwendungen durch.

Chime setup

So konfigurieren Sie einen Client für Amazon Q Developer in Chat-Anwendungen — Chime

Danach besteht der nächste Schritt darinCreate an Amazon SNS topic, Amazon Q Developer für Chime zu konfigurieren.

Führen Sie die Schritte unter Tutorial: Erste Schritte mit Amazon Chime im Administratorhandbuch für Amazon Q Developer in Chat-Anwendungen durch.

Amazon EventBridge für GuardDuty Ergebnisse verwenden

Mit erstellen Sie Regeln EventBridge, um die Ereignisse anzugeben, die Sie überwachen möchten. Diese Regeln spezifizieren auch die Zieldienste und -anwendungen, die automatisierte Aktionen ausführen können, wenn diese Ereignisse eintreten. Ein Ziel ist ein Ziel (eine Ressource oder ein Endpunkt), EventBridge an das ein Ereignis gesendet wird, wenn das Ereignis dem in der Regel definierten Ereignismuster entspricht. Jedes Ereignis ist ein JSON-Objekt, das dem EventBridge Schema für AWS Ereignisse entspricht und eine JSON-Darstellung eines Ergebnisses enthält. Sie können die Regel so anpassen, dass nur die Ereignisse gesendet werden, die bestimmte Kriterien erfüllen. Weitere Informationen finden Sie unter [Thema JSON-Schema]. Da die Ergebnisdaten als

EventBridgeEreignis strukturiert sind, können Sie die Ergebnisse mithilfe anderer Anwendungen, Dienste und Tools überwachen, verarbeiten und darauf reagieren.

Um Benachrichtigungen über GuardDuty Ergebnisse zu erhalten, die auf Ereignissen basieren, müssen Sie eine EventBridge Regel und ein Ziel für erstellen GuardDuty. Diese Regel EventBridge ermöglicht das Senden von Benachrichtigungen für GuardDuty generierte Ergebnisse an das in der Regel angegebene Ziel.

> **Note**
>
> EventBridge und CloudWatch Events sind derselbe zugrunde liegende Dienst und dieselbe API. EventBridge Enthält jedoch zusätzliche Funktionen, mit denen Sie Ereignisse von SaaS-Anwendungen (Software as a Service) und Ihren eigenen Anwendungen empfangen können. Da der zugrunde liegende Dienst und die API identisch sind, ist auch das Ereignisschema für GuardDuty Ergebnisse identisch.

Wie GuardDuty funktionieren archivierte und nicht archivierte Ergebnisse EventBridge

Bei Ergebnissen, die Sie manuell archivieren, werden die ersten und alle nachfolgenden Ergebnisse (die nach Abschluss der Archivierung generiert wurden) EventBridge anhand einer bestimmten Benachrichtigungshäufigkeit an folgende Empfänger gesendet. Weitere Informationen finden Sie unter Grundlegendes zur Häufigkeit von EventBridge Benachrichtigungen in GuardDuty.

Bei Ergebnissen, die automatisch archiviert werdenUnterdrückungsregeln, werden die ersten und alle nachfolgenden Vorkommen dieser Ergebnisse (die nach Abschluss der Archivierung generiert wurden) nicht an gesendet. EventBridge Sie können diese automatisch archivierten Ergebnisse in der GuardDuty Konsole einsehen.

Schema des Ereignisses

Ein Ereignismuster definiert, anhand welcher Daten bestimmt EventBridge wird, ob das Ereignis an das Ziel gesendet werden soll. Das EventBridge Ereignis für GuardDuty hat das folgende Format:

```
{
        "version": "0",
        "id": "cd2d702e-ab31-411b-9344-793ce56b1bc7",
        "detail-type": "GuardDuty Finding",
        "source": "aws.guardduty",
        "account": "111122223333",
```

```
 "time": "1970-01-01T00:00:00Z",
 "region": "us-east-1",
 "resources": [],
 "detail": {GUARDDUTY_FINDING_JSON_OBJECT}
}
```

Der *detail* Wert gibt die JSON-Details eines einzelnen Ergebnisses als Objekt zurück, im Gegensatz zur Rückgabe der gesamten Ergebnisantwortsyntax, die mehrere Ergebnisse innerhalb eines Arrays unterstützt.

Eine vollständige Liste aller in enthaltenen Parameter finden Sie GUARDDUTY_FINDING_JSON_OBJECT unter GetFindings. Der id-Parameter, der in der GUARDDUTY_FINDING_JSON_OBJECT angezeigt wird, ist die zuvor beschriebene Ergebnis-ID.

Eine EventBridge Regel für GuardDuty Ergebnisse erstellen

In den folgenden Verfahren wird erklärt, wie Sie mit der EventBridge Amazon-Konsole und dem AWS Command Line Interface (AWS CLI) eine EventBridge Regel für GuardDuty Ergebnisse erstellen. Die Regel erkennt EventBridge Ereignisse, die das Ereignisschema und das Muster für GuardDuty Ergebnisse verwenden, und sendet diese Ereignisse zur Verarbeitung an eine AWS Lambda Funktion.

AWS Lambda ist ein Rechendienst, mit dem Sie Code ausführen können, ohne Server bereitzustellen oder zu verwalten. Sie verpacken Ihren Code und laden ihn AWS Lambda als Lambda-Funktion hoch. AWS Lambda führt dann die Funktion aus, wenn die Funktion aufgerufen wird. Eine Funktion kann manuell von Ihnen, automatisch als Reaktion auf Ereignisse oder als Reaktion auf Anforderungen von Anwendungen oder Diensten aufgerufen werden. Informationen zum Erstellen und Abrufen und Lambda-Funktionen finden Sie im AWS Lambda -Entwicklerhandbuch.

Wählen Sie Ihre bevorzugte Methode, um eine EventBridge Regel zu erstellen, die Ihr GuardDuty Ergebnis an ein Ziel sendet.

Console

Gehen Sie wie folgt vor, um mit der EventBridge Amazon-Konsole eine Regel zu erstellen, die automatisch alle GuardDuty Findereignisse zur Verarbeitung an eine Lambda-Funktion sendet. Die Regel verwendet Standardeinstellungen für Regeln, die ausgeführt werden, wenn bestimmte Ereignisse empfangen werden. Einzelheiten zu Regeleinstellungen oder wie Sie eine Regel erstellen, die benutzerdefinierte Einstellungen verwendet, finden Sie im EventBridge Amazon-Benutzerhandbuch unter Regeln erstellen, die auf Ereignisse reagieren.

Bevor Sie diese Regel erstellen, erstellen Sie die Lambda-Funktion, die die Regel als Ziel verwenden soll. Wenn Sie die Regel erstellen, müssen Sie diese Funktion als Ziel für die Regel angeben. Ihr Ziel kann auch das SNS-Thema sein, das Sie zuvor erstellt haben. Weitere Informationen finden Sie unter Richten Sie ein Amazon SNS SNS-Thema und einen Endpunkt ein (E-Mail, Slack und Amazon Chime).

So erstellen Sie eine Ereignisregel mithilfe der Konsole

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie im Navigationsbereich unter Busse die Option Regeln aus.
3. Wählen Sie im Abschnitt Rules (Regeln) die Option Create rule (Regel erstellen) aus.
4. Gehen Sie auf der Detailseite Regel definieren wie folgt vor:
    a. Geben Sie für Rule name (Regelname) einen Namen für die Regel ein.
    b. (Optional) Geben Sie unter Beschreibung eine kurze Beschreibung der Regel ein.
    c. Stellen Sie sicher, dass für Event Bus die Option Standard ausgewählt ist und die Option Regel auf dem ausgewählten Event-Bus aktivieren aktiviert ist.
    d. Bei Regeltyp wählen Sie Regel mit einem Ereignismuster aus.
    e. Wenn Sie fertig sind, wählen Sie Next (Weiter) aus.
5. Gehen Sie auf der Seite Event-Pattern erstellen wie folgt vor:
    a. Wählen Sie als Ereignisquelle AWS Ereignisse oder EventBridge Partnerereignisse aus.
    b. (Optional) Sehen Sie sich für Beispielereignis ein Beispiel für ein Findereignis an GuardDuty , um zu erfahren, was ein Ereignis beinhalten könnte. Wählen Sie dazu AWS Ereignisse aus. Wählen Sie dann für Beispielereignisse die Option GuardDutyFinding aus.
    c. Option 1 — Verwenden von Pattern Form, einer Vorlage, die Folgendes EventBridge bietet

        Im Abschnitt Ereignismuster können Sie Folgendes tun:

        1. Wählen Sie als Erstellungsmethode die Option Musterformular verwenden aus.
        2. Wählen Sie für Ereignisquelle die Option AWS-Services aus.
        3. Wählen Sie für AWS-Service GuardDuty aus.
        4. Wählen Sie als Ereignistyp die Option GuardDuty Finding aus.

Wenn Sie fertig sind, wählen Sie Next (Weiter) aus.

d. Option 2 — Verwenden eines benutzerdefinierten Ereignismusters in JSON

Im Abschnitt Ereignismuster können Sie Folgendes tun:

1. Wählen Sie als Erstellungsmethode die Option Benutzerdefiniertes Muster (JSON-Editor) aus.
2. Fügen Sie im Feld Ereignismuster den folgenden benutzerdefinierten JSON-Code ein, der eine Warnung für mittlere, hohe und kritische Ergebnisse erstellt. Weitere Informationen finden Sie unter Schweregrad der Ergebnisse.

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "severity": [
      4,
      4.0,
      4.1,
      4.2,
      4.3,
      4.4,
      4.5,
      4.6,
      4.7,
      4.8,
      4.9,
      5,
      5.0,
      5.1,
      5.2,
      5.3,
      5.4,
      5.5,
      5.6,
      5.7,
```

```
        5.8,
        5.9,
        6,
        6.0,
        6.1,
        6.2,
        6.3,
        6.4,
        6.5,
        6.6,
        6.7,
        6.8,
        6.9,
        7,
        7.0,
        7.1,
        7.2,
        7.3,
        7.4,
        7.5,
        7.6,
        7.7,
        7.8,
        7.9,
        8,
        8.0,
        8.1,
        8.2,
        8.3,
        8.4,
        8.5,
        8.6,
        8.7,
        8.8,
        8.9,
        9,
        9.0,
        9.1,
        9.2,
        9.3,
        9.4,
        9.5,
        9.6,
        9.7,
```

```
      9.8,
      9.9,
      10,
      10.0
    ]
  }
}
```

Wenn Sie fertig sind, wählen Sie Next (Weiter) aus.

6. Option A — Auswahl AWS-Service — AWS Lambda als Ziel

   Gehen Sie auf der Seite Ziel (e) auswählen wie folgt vor:

   a. Wählen Sie für Zieltypen aus AWS-Service.

   b. Für Select a target (Ein Ziel auswählen), wählen die Option Lambda function (Lambda-Funktion) aus. Wählen Sie dann für Function die Lambda-Funktion aus, an die Sie Suchereignisse senden möchten.

   c. Geben Sie unter Configure version/alias die Versions- oder Aliaseinstellungen für die Lambda-Zielfunktion ein.

   d. (Optional) Geben Sie für Zusätzliche Einstellungen benutzerdefinierte Einstellungen ein, um anzugeben, welche Ereignisdaten Sie an die Lambda-Funktion senden möchten. Sie können auch angeben, wie Ereignisse behandelt werden sollen, die nicht erfolgreich an die Funktion übermittelt wurden.

   e. Wenn Sie fertig sind, wählen Sie Next (Weiter) aus.

7. Option B — Auswahl eines SNS-Themas als Ziel

   Gehen Sie auf der Seite Ziel (e) auswählen wie folgt vor:

   a. Wählen Sie für Zieltypen aus AWS-Service.

   b. Für Select a target (Wählen Sie ein Ziel aus), wählen Sie SNS-Thema aus. Wählen Sie dann für Zielstandort die passende Option aus, die auf Ihrem Zielort basiert. Wählen Sie unter Thema den Namen des SNS-Themas aus, das Sie erstellt haben.

   c. Erweitern Sie Additional settings (Zusätzliche Einstellungen). Wählen Sie für Zieleingabe konfigurieren die Option Eingangstransformator aus.

   d. Wählen Sie Configure input transformer (Eingabetransformator konfigurieren).

e. Kopieren Sie den folgenden Code und fügen Sie ihn in das Feld Eingabepfad im Abschnitt Zieleingangstransformator ein.

```
{
    "severity": "$.detail.severity",
    "Account_ID": "$.detail.accountId",
    "Finding_ID": "$.detail.id",
    "Finding_Type": "$.detail.type",
    "region": "$.region",
    "Finding_Description": "$.detail.description"
}
```

f. Kopieren Sie den folgenden Code und fügen Sie ihn in das Feld Vorlage ein, um die E-Mail zu formatieren.

```
"You have a severity <severity> GuardDuty finding type <Finding_Type> in the
 <region> Region."
"Finding Description:"
"<Finding_Description>. "
"For more details open the GuardDuty console at https://
console.aws.amazon.com/guardduty/home?region=<region>#/findings?search=id
%3D<Finding_ID>"
```

8. Geben Sie auf der Seite „Tags konfigurieren“ optional ein oder mehrere Tags ein, die der Regel zugewiesen werden sollen. Klicken Sie anschließend auf Weiter.
9. Überprüfen Sie auf der Seite Überprüfen und erstellen die Einstellungen der Regel und stellen Sie sicher, dass sie korrekt sind.

   Um eine Einstellung zu ändern, wählen Sie in dem Abschnitt, der die Einstellung enthält, Bearbeiten aus und geben Sie dann die richtige Einstellung ein. Sie können auch die Navigationsregisterkarten verwenden, um zu der Seite zu gelangen, die eine Einstellung enthält.
10. Wenn Sie mit der Überprüfung der Einstellungen fertig sind, wählen Sie Regel erstellen aus.

API

Das folgende Verfahren zeigt, wie Sie mithilfe von AWS CLI Befehlen eine EventBridge Regel und ein Ziel für GuardDuty erstellen. Das Verfahren zeigt Ihnen insbesondere, wie Sie eine Regel

erstellen, die es EventBridge ermöglicht, Ereignisse für alle GuardDuty generierten Ergebnisse an eine AWS Lambda Funktion als Ziel für die Regel zu senden.

> **Note**
>
> In diesem Beispiel verwenden wir eine Lambda-Funktion als Ziel für die EventBridge auslösende Regel. Sie können auch andere AWS Ressourcen als auszulösende Ziele konfigurieren. EventBridge GuardDuty und EventBridge unterstützt die folgenden Zieltypen: Amazon EC2 EC2-Instances, Amazon Kinesis Kinesis-Streams, Amazon ECS-Aufgaben, AWS Step Functions Zustandsmaschinen, den `run` Befehl und integrierte Ziele. Weitere Informationen finden Sie PutTargetsin der Amazon EventBridge API-Referenz.

Erstellen von Regeln und Zielen

1. Führen Sie den folgenden EventBridge CLI-Befehl aus, EventBridge um eine Regel zu erstellen, die das Senden von Ereignissen für alle GuardDuty generierten Ergebnisse ermöglicht.

   ```
   aws events put-rule --name your-rule-name --event-pattern "{\"source\":
   [\"aws.guardduty\"]}"
   ```

   Sie können Ihre Regel weiter anpassen, sodass sie anweist, Ereignisse nur für eine Teilmenge der GuardDuty-generated Ergebnisse EventBridge zu senden. Diese Untergruppe basiert auf dem/den in der Regel angegebenen Ergebnisattribut(en). Verwenden Sie beispielsweise den folgenden CLI-Befehl, um eine Regel zu erstellen, die es ermöglicht EventBridge , nur Ereignisse für die GuardDuty Ergebnisse mit dem Schweregrad 5 oder 8 zu senden:

   ```
   aws events put-rule --name your-rule-name --event-pattern "{\"source\":
   [\"aws.guardduty\"],\"detail-type\":[\"GuardDuty Finding\"],\"detail\":
   {\"severity\":[5,8]}}"
   ```

   Zu diesem Zweck können Sie alle Eigenschaftswerte verwenden, die im JSON für GuardDuty Ergebnisse verfügbar sind.
2. Führen Sie den folgenden CloudWatch CLI-Befehl aus, um eine Lambda-Funktion als Ziel für die Regel anzuhängen, die Sie in Schritt 1 erstellt haben.

```
aws events put-targets --rule your-target-name --targets
 Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:your_function
```

Stellen Sie sicher, dass Sie `your-target-name` den obigen Befehl durch Ihre tatsächliche Lambda-Funktion für die GuardDuty Ereignisse ersetzen.

3. Führen Sie den folgenden Lambda-CLI-Befehl aus, um die erforderlichen Berechtigungen zum Aufrufen des Ziels hinzuzufügen.

```
aws lambda add-permission --function-name your-target-name --statement-id 1 --
action 'lambda:InvokeFunction' --principal events.amazonaws.com
```

Stellen Sie sicher, dass Sie `your_function` den obigen Befehl durch Ihre tatsächliche Lambda-Funktion für die GuardDuty Ereignisse ersetzen.

EventBridge Regel für Umgebungen mit GuardDuty mehreren Konten

Wenn Sie ein delegiertes GuardDuty Administratorkonto verwenden, können Sie die in den Mitgliedskonten generierten Ereignisse einsehen und mithilfe anderer Anwendungen und Dienste Maßnahmen ergreifen. EventBridge Regeln in Ihrem Administratorkonto werden basierend auf den entsprechenden Ergebnissen aus Ihren Mitgliedskonten ausgelöst. Wenn Sie EventBridge in Ihrem Administratorkonto Benachrichtigungen für die Suche einrichten, erhalten Sie Benachrichtigungen über Ergebnisse sowohl von Ihrem Konto als auch von Ihren Mitgliedskonten. Sie können es beispielsweise verwenden, EventBridge um bestimmte Arten von Ergebnissen an eine Lambda-Funktion zu senden, die die Daten verarbeitet und an Ihr SIEM-System (Security Incident and Event Management) sendet.

Sie können das Mitgliedskonto, aus dem das GuardDuty Ergebnis stammt, anhand des `accountId` Felds mit den JSON-Details des Ergebnisses identifizieren. Um eine benutzerdefinierte Ereignisregel für bestimmte Mitgliedskonten zu erstellen, erstellen Sie eine neue Regel und verwenden Sie die folgende Vorlage unter Ereignismuster. *123456789012*Ersetzen Sie es durch das Konto `accountId` des Mitgliedskontos, für das Sie das Ereignis auslösen möchten.

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
```

```
    "GuardDuty Finding"
  ],
  "detail": {
    "accountId": [
      "123456789012"
    ]
  }
}
```

> **Note**
>
> In diesem Beispiel wird eine Regel erstellt, die allen Ergebnissen der angegebenen Konto-ID entspricht. Sie können mehrere Konto-IDs angeben, indem Sie sie gemäß der JSON-Syntax durch Kommas trennen.

Grundlegendes zu CloudWatch Protokollen und Gründen für das Überspringen von Ressourcen beim Scan von Malware Protection for EC2

GuardDuty Malware Protection for EC2 veröffentlicht Ereignisse in Ihrer Amazon-Protokollgruppe// malware scan-events. CloudWatch aws/guardduty Für jedes Ereignis im Zusammenhang mit dem Malware-Scan können Sie den Status und das Scanergebnis Ihrer betroffenen Ressourcen überwachen. Bestimmte Amazon EC2-Ressourcen und Amazon EBS-Volumes wurden möglicherweise während des Malware-Schutzes für EC2 übersprungen.

CloudWatch Audit-Protokolle in Malware Protection for EC2 GuardDuty

In der Protokollgruppe/aws/guardduty CloudWatch /malware scan-events werden drei Arten von Scanereignissen unterstützt.

Name des Ereignisses „Schutz vor Schadsoft ware“ für EC2-Scan	Erklärung
`EC2_SCAN_STARTED`	Wird erstellt, wenn ein GuardDuty Malware-Schutz für EC2 den Malware-Scanvorgang

Name des Ereignisses „Schutz vor Schadsoftware“ für EC2-Scan	Erklärung
	initiiert, z. B. die Erstellung eines Snapshots eines EBS-Volumes vorbereitet.
`EC2_SCAN_COMPLETED`	Wird erstellt, wenn der Scan von GuardDuty Malware Protection for EC2 für mindestens eines der EBS-Volumes der betroffenen Ressource abgeschlossen ist. Dieses Ereignis umfasst auch das `snapshotId` , das zum gescannten EBS-Volume gehört. Nach Abschluss des Scans lautet das Scanergebnis entweder `CLEAN`, `THREATS_FOUND` oder `NOT_SCANNED` .
`EC2_SCAN_SKIPPED`	Wird erstellt, wenn der Scan von GuardDuty Malware Protection for EC2 alle EBS-Volumes der betroffenen Ressource überspringt. Um den Grund für das Überspringen zu ermitteln, wählen Sie das entsprechende Ereignis aus und sehen Sie sich die Details an. Weitere Informationen zu den Gründen für das Überspringen finden Sie unter Gründe für das Überspringen von Ressourcen beim Malware-Scan weiter unten.

> **Note**
>
> Wenn Sie eine verwenden AWS Organizations, werden CloudWatch Protokollereignisse von Mitgliedskonten in Organisationen sowohl im Administratorkonto als auch in der Protokollgruppe des Mitgliedskontos veröffentlicht.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um CloudWatch Ereignisse anzuzeigen und abzufragen.

Console

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Protokolle die Option Protokollgruppen. Wählen Sie die Protokollgruppe/aws/guardduty/malware scan-events aus, um die Scanereignisse für GuardDuty Malware Protection for EC2 anzuzeigen.

   Um eine Abfrage auszuführen, wählen Sie Log Insights.

   Informationen zum Ausführen einer Abfrage finden Sie unter Analysieren von Protokolldaten mit CloudWatch Logs Insights im Amazon-Benutzerhandbuch. CloudWatch
3. Wählen Sie Scan-ID, um die Details der betroffenen Ressourcen und Malware-Erkenntnisse zu überwachen. Sie können beispielsweise die folgende Abfrage ausführen, um die CloudWatch Protokollereignisse mithilfe von zu filtern`scanId`. Stellen Sie sicher, dass Sie Ihr eigenes gültiges Passwort verwenden*`scan-id`*.

   ```
   fields @timestamp, @message, scanRequestDetails.scanId as scanId
   | filter scanId like "77a6f6115da4bd95f4e4ca398492bcc0"
   | sort @timestamp asc
   ```

API/CLI

- Informationen zur Arbeit mit Protokollgruppen finden Sie AWS CLI im CloudWatch Amazon-Benutzerhandbuch unter Suchen nach Protokolleinträgen mithilfe von.

  Wählen Sie die Protokollgruppe/aws/guardduty/malware scan-events, um die Scanereignisse für GuardDuty Malware Protection for EC2 anzuzeigen.
- Informationen zum Anzeigen und Filtern von Protokollereignissen finden Sie unter GetLogEvents bzw. in der FilterLogEvents Amazon-API-Referenz. CloudWatch

GuardDuty Malware-Schutz für die Aufbewahrung von EC2-Protokollen

Die standardmäßige Aufbewahrungsdauer für die Protokollgruppe/aws/guardduty/malware scan-events beträgt 90 Tage. Danach werden die Protokollereignisse automatisch gelöscht. Informationen zum Ändern der Protokollaufbewahrungsrichtlinie für Ihre CloudWatch Protokollgruppe finden Sie

unter Ändern der Aufbewahrung von Protokolldaten in CloudWatch Protokollen im CloudWatch Amazon-Benutzerhandbuch oder PutRetentionPolicy in der Amazon-API-Referenz. CloudWatch

Gründe für das Überspringen von Ressourcen beim Malware-Scan

Bei Ereignissen im Zusammenhang mit dem Malware-Scan wurden möglicherweise bestimmte EC2-Ressourcen und EBS-Volumes während des Scanvorgangs übersprungen. In der folgenden Tabelle sind die Gründe aufgeführt, warum GuardDuty Malware Protection for EC2 die Ressourcen möglicherweise nicht scannt. Verwenden Sie gegebenenfalls die vorgeschlagenen Schritte, um diese Probleme zu beheben, und scannen Sie diese Ressourcen, wenn GuardDuty Malware Protection for EC2 das nächste Mal einen Malware-Scan initiiert. Die anderen Probleme dienen dazu, Sie über den Verlauf der Ereignisse zu informieren, und sind nicht umsetzbar.

Gründe für das Überspringen	Erklärung	Vorgeschlagene Schritte
`RESOURCE_NOT_FOUND`	Die zum Initiieren des On-Demand-Malware-Scans `resourceArn` bereitgestellte Datei wurde in Ihrer AWS Umgebung nicht gefunden.	Überprüfen Sie den `resourceArn` Ihres Amazon-EC 2-Instance- oder Container-Workloads und versuchen Sie es erneut.
`ACCOUNT_INELIGIBLE`	Die AWS Konto-ID, von der aus Sie versucht haben, einen On-demand Malware-Scan zu starten, wurde nicht aktiviert GuardDuty.	Stellen Sie sicher, dass GuardDuty dies für dieses AWS Konto aktiviert ist. Wenn Sie ein neues aktivieren GuardDuty , AWS-Region kann die Synchronisierung bis zu 20 Minuten dauern.
`UNSUPPORTED_KEY_ENCRYPTION`	GuardDuty Malware Protection for EC2 unterstützt Volumes,	Ersetzen Sie Ihren Verschlüsselungsschlüssel durch einen

Gründe für das Überspringen	Erklärung	Vorgeschlagene Schritte	
	die sowohl unverschlüsselt als auch mit einem vom Kunden verwalteten Schlüssel verschlüsselt sind. Das Scannen von EBS-Volumes, die mit der Amazon-EBS-Verschlüsselung verschlüsselt wurden, wird nicht unterstützt. Derzeit gibt es einen regionalen Unterschied, bei dem dieser Grund für das Überspringen nicht zutrifft. Weitere Informationen dazu finden Sie AWS-Regionen unterRegion-specific Verfügbarkeit von Funktionen.	vom Kunden verwalteten Schlüssel. Weitere Informationen zu den GuardDuty unterstützten Verschlüsselungstypen finden Sie unterUnterstützte Amazon EBS-Volumes für den Malware-Scan.	

Gründe für das Überspringen	Erklärung	Vorgeschlagene Schritte	
`EXCLUDED_BY_SCAN_SETTINGS`	Die EC2-Instance oder das EBS-Volume wurde beim Malware-Scan ausgeschlossen. Es gibt zwei Möglichkeiten: Entweder wurde das Tag zur Einschließen-Liste hinzugefügt, aber die Ressource ist nicht mit diesem Tag verknüpft, das Tag wurde der Ausschließen-Liste hinzugefügt und die Ressource ist mit diesem Tag verknüpft, oder das `GuardDuty Excluded` -Tag ist für diese Ressource auf `true` gesetzt.	Aktualisieren Sie Ihre Scan-Optionen oder die Ihrer Amazon-EC2-Ressource zugeordneten Tags. Weitere Informationen finden Sie unter Scan-Optionen mit benutzerdefinierten Tags.	
`UNSUPPORTED_VOLUME_SIZE`	Das Volumen ist größer als 2048 GB.	Nicht umsetzbar.	
`NO_VOLUMES_ATTACHED`	GuardDuty Malware Protection for EC2 hat die Instance in Ihrem Konto gefunden, aber es wurde kein EBS-Volume an diese Instance angehängt, um mit dem Scan fortzufahren.	Nicht umsetzbar.	

Gründe für das Überspringen	Erklärung	Vorgeschlagene Schritte	
UNABLE_TO_SCAN	Es ist ein interner Servicefehler.	Nicht umsetzbar.	
SNAPSHOT_NOT_FOUND	Die von den EBS-Volumes erstellten und mit dem Dienstkonto geteilten Snapshots wurden nicht gefunden, und GuardDuty Malware Protection for EC2 konnte den Scan nicht fortsetzen.	Stellen Sie sicher CloudTrail , dass die Snapshots nicht absichtlich entfernt wurden.	
SNAPSHOT_QUOTA_REACHED	Sie haben das maximale Volumen erreicht, das für Snapshots für jede Region zulässig ist. Dadurch wird verhindert, dass Snapshots nicht nur gespeichert, sondern auch neue erstellt werden.	Sie können entweder alte Snapshots entfernen oder eine Erhöhung des Kontingents beantragen. Das Standardlimit für Snapshots pro Region und wie Sie eine Erhöhung des Kontingents beantragen können, finden Sie unter Service Quotas im Allgemeinen Referenzhandbuch von AWS .	

Gründe für das Überspringen	Erklärung	Vorgeschlagene Schritte	
`MAX_NUMBER_OF_ATTACHED_VOLUMES_REACHED`	Mehr als 11 EBS-Volumes wurden an eine EC2-Instance angehängt. GuardDuty Malware Protection for EC2 hat die ersten 11 EBS-Volumes gescannt und durch alphabetische Sortierung ermittelt. `deviceName`	Nicht umsetzbar.	

Gründe für das Überspringen	Erklärung	Vorgeschlagene Schritte	
`UNSUPPORTED_PRODUCT_CODE_TYPE`	GuardDuty kann die meisten Instanzen mit as scannen. `productCode` `marketplace` Einige Marketplace-Instances sind möglicherweise nicht zum Scannen geeignet. GuardDuty überspringt solche Fälle und protokolliert den Grund als`UNSUPPORTED_PRODUCT_CODE_TYPE` . Diese Unterstützung ist je nach Region AWS GovCloud (US) und Region China unterschiedlich. Weitere Informationen finden Sie unter Region-specific Verfügbarkeit von Funktionen. Weitere Informationen finden Sie unter Bezahlte AMIs im Amazon EC2-Benutzerhandbuch. Weitere Informationen zu `productCo`	Nicht umsetzbar.	

Gründe für das Überspringen	Erklärung	Vorgeschlagene Schritte	
	de finden Sie unter ProductCode in der Amazon-EC2-API-Referenz.		

Falschmeldungen in Malware Protection for EC2 melden

GuardDuty Malware Protection for EC2-Scans können eine harmlose Datei in Ihrer Amazon EC2 EC2-Instance oder Ihrem Container-Workload als bösartig oder schädlich identifizieren. Um Ihre Erfahrung mit Malware Protection for EC2 und dem GuardDuty Service zu verbessern, können Sie falsch positive Ergebnisse melden, wenn Sie der Meinung sind, dass eine bei einem Scan als bösartig oder schädlich identifizierte Datei in Wirklichkeit keine Malware enthält.

Um das Ergebnis eines Amazon EC2-Malware-Scans als falsch positiv zu melden

Um den Vorgang einzuleiten, wenden Sie sich an Support. Gehen Sie wie folgt vor, um Details zur gescannten Ressource bereitzustellen:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie EC2-Malware-Scans.
3. Wählen Sie einen Scan aus, um die zugehörige Erkenntnis-ID anzuzeigen.
4. Geben Sie die Erkenntnis-ID ein. Sie müssen auch den SHA-256 Hash der Datei angeben. Dies ist erforderlich, um sicherzustellen, dass GuardDuty Malware Protection for EC2 die richtige Datei erhalten hat.
5. Das Support Team stellt Ihnen eine vorsignierte Amazon Simple Storage Service (Amazon S3) -URL zur Verfügung, mit der Sie die potenziell schädliche Datei und den SHA-256 Hash hochladen können. Informationen zu den Schritten zum Hochladen des gescannten Objekts finden Sie unter Hochladen von Objekten mit vorsignierten URLs im Amazon S3 S3-Benutzerhandbuch.
6. Nachdem Sie die Datei hochgeladen haben, informieren Sie das Support Team.

   Sie Support erhalten nach Erhalt der Datei eine Bestätigung. Die Mitglieder des GuardDuty Serviceteams werden Ihre Einreichung analysieren und geeignete Maßnahmen ergreifen, um

Ihre Erfahrung mit Malware Protection for EC2 und dem Service zu verbessern. GuardDuty Das Support Team wird Sie weiterhin über den aktuellen Stand Ihres Falls informieren. GuardDuty bewahrt Ihr S3-Objekt nicht länger als 30 Tage auf.

S3-Objektscanergebnis in Malware Protection for S3 als falsch positiv melden

Ein Scan von Malware Protection for S3 kann ein Objekt als potenziell bösartig oder schädlich identifizieren. Wenn Sie glauben, dass das angegebene S3-Objekt keine Malware enthält, melden Sie dieses Malware-Scan-Ergebnis als falsch positiv.

Sie können einen falsch positiven Bericht einreichen, auch wenn Sie Malware Protection for S3 unabhängig verwenden. In diesem Fall GuardDuty ist es nicht darauf ausgelegt, einen Befund zu generieren. Hinweise zur Überprüfung des Scanstatus und des Ergebnisstatus finden Sie unterÜberwachung von S3-Objektscans.

So melden Sie das Ergebnis eines Malware-S3-Objekts als falsch positiv

Um den Vorgang einzuleiten, wenden Sie sich an Support. Gehen Sie wie folgt vor, um Details zum gescannten S3-Objekt bereitzustellen:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie je nach Anwendungsfall die entsprechenden Schritte aus:

   Using Malware Protection for S3 with GuardDuty

   1. Wählen Sie im Navigationsbereich Findings aus.
   2. Wählen Sie auf der Seite Ergebnisse das falsch positive Ergebnis aus, um dessen Details anzuzeigen.
   3. Wenn Sie die Ergebnisdetails überprüfen, geben Sie die Such-ID, die Region, den Namen des geschützten S3-Buckets und den Schlüssel des gescannten Objekts an.

      Geben Sie in den Elementpfaddetails den Hash des Objekts an. Dies ist erforderlich, um sicherzustellen, GuardDuty dass ich die richtige Datei erhalten habe.

Using Malware Protection for S3 independently

Geben Sie den Namen des geschützten S3-Buckets, den Namen des gescannten Objekts und den an AWS-Region.

3. Das Support Team stellt Ihnen eine vorsignierte Amazon Simple Storage Service (Amazon S3) -URL zur Verfügung, mit der Sie die potenziell schädliche Datei und den Hash hochladen können. Informationen zu den Schritten zum Hochladen des gescannten Objekts finden Sie unter Hochladen von Objekten mit vorsignierten URLs im Amazon S3 S3-Benutzerhandbuch.
4. Informieren Sie das Team, nachdem Sie das S3-Objekt hochgeladen haben. Support

Sie Support erhalten eine Bestätigung über den Empfang des Objekts. Die Mitglieder des GuardDuty Serviceteams werden Ihre Einreichung analysieren und geeignete Maßnahmen ergreifen, um Ihre Erfahrung mit Malware Protection for S3 und dem GuardDuty Service zu verbessern. Das Support Team wird Sie weiterhin über den aktuellen Stand Ihres Falls informieren. GuardDuty bewahrt Ihr S3-Objekt nicht länger als 30 Tage auf.

Falschmeldungen in Malware Protection for Backup melden

Um Ihre Erfahrung mit GuardDuty Malware Protection for Backup zu verbessern, können Sie potenzielle Fehlalarme und Falschmeldungen melden.

Um ein potenzielles falsch positives oder falsch negatives Ergebnis zu melden, das in Malware Protection for Backup identifiziert wurde

Um den Vorgang einzuleiten, wenden Sie sich an Support. Gehen Sie wie folgt vor, um Details zur gescannten Ressource bereitzustellen:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie Malware-Scans.
3. Wählen Sie einen Scan aus, um die zugehörige Erkenntnis-ID anzuzeigen.
4. Geben Sie die Erkenntnis-ID ein. Sie müssen auch den SHA-256 Hash der Datei angeben. Dies ist erforderlich, um sicherzustellen, GuardDuty dass ich die richtige Datei erhalten habe. Bitte geben Sie auch die Region an, aus der Sie die Probe liefern werden.

5. Das Support Team stellt Ihnen eine vorsignierte Amazon Simple Storage Service (Amazon S3) -URL zur Verfügung, mit der Sie die potenziell schädliche Datei und den SHA-256 Hash hochladen. Informationen zu den Schritten zum Hochladen der gescannten Ressource finden Sie unter Hochladen von Objekten mit vorsignierten URLs im Amazon S3 S3-Benutzerhandbuch.
6. Nachdem Sie die Datei hochgeladen haben, informieren Sie das Support Team.

   Sie Support erhalten nach Erhalt der Datei eine Bestätigung. Die Mitglieder des GuardDuty Serviceteams werden Ihre Einreichung analysieren und geeignete Maßnahmen ergreifen, um Ihre Erfahrung mit Malware Protection for EC2 zu verbessern. Das Support Team wird Sie weiterhin über den Status Ihres Falls informieren. GuardDuty bewahrt Ihr S3-Objekt nicht länger als 30 Tage auf.

Behebung erkannter GuardDuty Sicherheitslücken

Amazon GuardDuty generiert Ergebnisse, die auf potenzielle Sicherheitslücken im Zusammenhang mit der GuardDuty grundlegenden Bedrohungserkennung und speziellen Schutzplänen hinweisen. In den folgenden Abschnitten werden die empfohlenen Schritte zur Behebung für alle Szenarien beschrieben. Falls es alternative Abhilfeszenarien gibt, werden diese in den Beschreibungen für jeden Befundtyp beschrieben. Sie können auf die vollständigen Informationen zu einem Erkenntnistyp zugreifen, indem Sie ihn aus der Tabelle für aktive Erkenntnistypen auswählen.

Inhalt

- Behebung einer potenziell kompromittierten Amazon EC2-Instance
- Behebung eines potenziell kompromittierten S3-Buckets
- Behebung eines potenziell bösartigen S3-Objekts
- Behebung eines potenziell kompromittierten EBS-Snapshots
- Behebung eines potenziell kompromittierten EC2-AMI
- Behebung eines potenziell kompromittierten EC2-Wiederherstellungspunkts
- Behebung eines potenziell kompromittierten S3-Wiederherstellungspunkts
- Behebung eines potenziell kompromittierten ECS-Clusters
- Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten
- Behebung eines potenziell kompromittierten Standalone-Containers
- Behebung der EKS-Schutzfeststellungen
- Korrigieren von Erkenntnissen der Laufzeitüberwachung
- Behebung einer potenziell gefährdeten Datenbank
- Behebung einer potenziell gefährdeten Lambda-Funktion

Behebung einer potenziell kompromittierten Amazon EC2-Instance

Wenn Suchtypen GuardDuty generiert werden, die auf potenziell kompromittierte Amazon EC2-Ressourcen hinweisen, dann ist Ihre Ressource Instance. Mögliche Suchtypen könnten seinEC2-Erkenntnistypen,GuardDuty Findetypen für die Laufzeitüberwachung, oder. Malware-Schutz für EC2-Suchtypen Wenn das Verhalten, das den Befund verursacht hat, in Ihrer Umgebung erwartet wurde, sollten Sie die Verwendung in Betracht ziehenUnterdrückungsregeln.

Führen Sie die folgenden Schritte aus, um die potenziell kompromittierte Amazon EC2-Instance zu reparieren:

1. Identifizieren Sie die potenziell gefährdete Amazon EC2-Instance

   Untersuchen Sie die potenziell kompromittierte Instance auf Malware und entfernen Sie sämtliche gefundene Malware. Sie können On-demand Malware-Scan in GuardDuty verwenden, um Malware in der potenziell gefährdeten EC2-Instance zu identifizieren oder AWS Marketplace überprüfen, ob es hilfreiche Partnerprodukte zur Identifizierung und Entfernung von Malware gibt.

2. Isolieren Sie die potenziell gefährdete Amazon EC2-Instance

   Verwenden Sie nach Möglichkeit die folgenden Schritte, um die potenziell gefährdete Instance zu isolieren:

   1. Erstellen Sie eine dedizierte Isolations-Sicherheitsgruppe. Eine isolierte Sicherheitsgruppe sollte nur eingehenden und ausgehenden Zugriff von bestimmten IP-Adressen aus haben. Stellen Sie sicher, dass es keine Regel für eingehenden oder ausgehenden Datenverkehr gibt, die den Datenverkehr zulässt. `0.0.0.0/0 (0-65535)`
   2. Ordnen Sie die Isolations-Sicherheitsgruppe dieser Instanz zu.
   3. Entfernen Sie alle Sicherheitsgruppenzuordnungen mit Ausnahme der neu erstellten Isolations-Sicherheitsgruppe aus der potenziell gefährdeten Instanz.

   > **Note**
   >
   > Die bestehenden getrackten Verbindungen werden nicht aufgrund eines Wechsels der Sicherheitsgruppen beendet — nur zukünftiger Datenverkehr wird von der neuen Sicherheitsgruppe wirksam blockiert.
   > Informationen zum Blockieren von weiterem Datenverkehr von verdächtigen bestehenden Verbindungen finden Sie im Incident Response Playbook unter Durchsetzen von NACLs auf Netzwerkbasis, IoCs um weiteren Datenverkehr zu verhindern.

3. Identifizieren Sie die Quelle der verdächtigen Aktivität.

   Wenn Malware erkannt wird, identifizieren und beenden Sie anhand des Erkennungstyps in Ihrem Konto die potenziell nicht autorisierte Aktivität auf Ihrer EC2-Instance. Dies kann Aktionen wie das Schließen aller offenen Ports, das Ändern von Zugriffsrichtlinien und das Aktualisieren von Anwendungen zur Behebung von Schwachstellen erfordern.

Wenn Sie nicht in der Lage sind, unbefugte Aktivitäten auf Ihrer potenziell gefährdeten EC2-Instance zu identifizieren und zu stoppen, empfehlen wir Ihnen, die kompromittierte EC2-Instance zu beenden und sie bei Bedarf durch eine neue Instance zu ersetzen. Nachfolgend finden Sie weitere Ressourcen zum Schützen Ihrer EC2-Instances:

- Abschnitte „Sicherheit und Netzwerk“ im Dokument Bewährte Methoden für Amazon EC2.
- Amazon EC2-Sicherheitsgruppen für Linux-Instances.
- Sicherheit in Amazon EC2
- Tipps zum Sichern Ihrer EC2-Instances (Linux)
- AWS Bewährte Sicherheitsmethoden
- AWS Technischer Leitfaden zur Reaktion auf Sicherheitsvorfälle.

4. Durchsuchen AWS re:Post

   AWS re:PostSuchen Sie nach weiterer Unterstützung.

5. Reichen Sie eine Anfrage für technischen Support ein

   Wenn Sie ein Premium-Support-Paket abonniert haben, können Sie eine Anfrage für den technischen Support senden.

Behebung eines potenziell kompromittierten S3-Buckets

Wenn es GuardDuty generiert wirdGuardDuty S3 Schutzsuchtypen, deutet dies darauf hin, dass Ihre Amazon S3-Buckets kompromittiert wurden. Wenn das Verhalten, das den Befund verursacht hat, in Ihrer Umgebung erwartet wurde, sollten Sie eine Erstellung in Betracht ziehen. Unterdrückungsregeln Wenn dieses Verhalten nicht erwartet wurde, folgen Sie diesen empfohlenen Schritten, um einen potenziell gefährdeten Amazon S3-Bucket in Ihrer AWS Umgebung zu beheben:

1. Identifizieren Sie die potenziell gefährdete S3-Ressource.

   Ein GuardDuty Ergebnis für S3 listet den zugehörigen S3-Bucket, seinen Amazon-Ressourcennamen (ARN) und seinen Besitzer in den Ergebnisdetails auf.

2. Identifizieren Sie die Quelle der verdächtigen Aktivität und des verwendeten API-Aufrufs.

   Der verwendete API-Aufruf wird in den Ergebnisdetails als `API` aufgelistet. Bei der Quelle handelt es sich um einen IAM-Prinzipal (entweder eine IAM-Rolle, ein IAM-Benutzer oder ein IAM-Konto) und identifizierende Details werden in der Erkenntnis aufgeführt. Je nach Quelltyp

sind Informationen zur Remote-IP-Adresse oder zur Quelldomain verfügbar, anhand derer Sie beurteilen können, ob die Quelle autorisiert wurde. Wenn das Ergebnis Anmeldeinformationen einer Amazon EC2-Instance beinhaltete, werden die Details für diese Ressource ebenfalls enthalten sein.

3. Stellen Sie fest, ob die Anrufquelle autorisiert war, auf die identifizierte Ressource zuzugreifen.

   Denken Sie zum Beispiel an Folgendes:

   - Wenn ein IAM-Benutzer beteiligt war, ist es möglich, dass seine Anmeldeinformationen möglicherweise kompromittiert wurden? Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.
   - Wenn eine API von einem Prinzipal aufgerufen wurde, der diesen API-Typ noch nie aufgerufen hat, benötigt diese Quelle dann Zugriffsberechtigungen für diesen Vorgang? Können die Bucket-Berechtigungen weiter eingeschränkt werden?
   - Wenn der Zugriff anhand des Benutzernamens `ANONYMOUS_PRINCIPAL` mit dem Benutzertyp `AWSAccount` erkannt wurde, bedeutet dies, dass der Bucket öffentlich ist und darauf zugegriffen wurde. Sollte dieser Bucket öffentlich sein? Falls nicht, finden Sie in den folgenden Sicherheitsempfehlungen alternative Lösungen für die gemeinsame Nutzung von S3-Ressourcen.
   - Wenn der Zugriff über einen erfolgreichen `PreflightRequest`-Aufruf erfolgte, wird anhand des Benutzernamens `ANONYMOUS_PRINCIPAL` mit dem Benutzertyp `AWSAccount` angezeigt, dass für den Bucket eine CORS-Richtlinie (Cross-Origin Resource Sharing) festgelegt wurde. Sollte dieser Bucket eine CORS-Richtlinie haben? Falls nicht, stellen Sie sicher, dass der Bucket nicht versehentlich öffentlich ist, und finden Sie in den folgenden Sicherheitsempfehlungen alternative Lösungen für die gemeinsame Nutzung von S3-Ressourcen. Weitere Informationen zu CORS und Amazon S3 finden Sie unter Cross-Origin Resource Sharing (CORS) verwenden im Benutzerhandbuch zu S3.

4. Stellen Sie fest, ob der S3-Bucket sensible Daten enthält.

   Verwenden Sie Amazon Macie, um zu ermitteln, ob der S3-Bucket sensible Daten, wie persönlich identifizierbare Informationen (PII), Finanzdaten oder Anmeldeinformationen enthält. Wenn die automatische Erkennung sensibler Daten für Ihr Macie-Konto aktiviert ist, überprüfen Sie die Details des S3-Buckets, um den Inhalt Ihres S3-Buckets besser zu verstehen. Wenn dieses Feature für Ihr Macie-Konto deaktiviert ist, empfehlen wir, es zu aktivieren, um Ihre Bewertung zu beschleunigen. Alternativ können Sie einen Discovery-Job für sensible Daten erstellen und ausführen, um die Objekte des S3-Buckets auf sensible Daten zu untersuchen. Weitere Informationen finden Sie unter Aufspüren sensibler Daten mit Macie.

Wenn der Zugriff autorisiert wurde, können Sie die Erkenntnis ignorieren. In der https://console.aws.amazon.com/guardduty/ Konsole können Sie Regeln einrichten, um einzelne Ergebnisse vollständig zu unterdrücken, sodass sie nicht mehr angezeigt werden. Weitere Informationen finden Sie unter Unterdrückungsregeln in GuardDuty.

Wenn Sie feststellen, dass Ihre S3-Daten offengelegt wurden oder von Unbefugten abgerufen wurden, lesen Sie die folgenden S3-Sicherheitsempfehlungen, um die Berechtigungen zu verschärfen und den Zugriff einzuschränken. Welche Lösungen für die Behebung geeignet sind, hängt von den Anforderungen Ihrer spezifischen Umgebung ab.

Empfehlungen, die auf spezifischen S3-Bucket-Zugriffsanforderungen basieren

Die folgende Liste enthält Empfehlungen, die auf bestimmten Amazon S3-Bucket-Zugriffsanforderungen basieren:

- Um den öffentlichen Zugriff auf Ihre S3-Datennutzung zentral einzuschränken, blockieren Sie mit S3 den öffentlichen Zugriff. Die Einstellungen zur Sperrung des öffentlichen Zugriffs können für Access Points, Buckets und AWS Konten mithilfe von vier verschiedenen Einstellungen aktiviert werden, um die Granularität des Zugriffs zu kontrollieren. Weitere Informationen finden Sie im Amazon S3-Benutzerhandbuch unter Einstellungen für öffentlichen Zugriff blockieren.
- AWS Mithilfe von Zugriffsrichtlinien können Sie steuern, wie IAM-Benutzer auf Ihre Ressourcen zugreifen können oder wie auf Ihre Buckets zugegriffen werden kann. Weitere Informationen finden Sie unter Verwenden von Bucket-Richtlinien und Benutzerrichtlinien im Amazon S3-Benutzerhandbuch.

  Darüber hinaus können Sie Virtual Private Cloud (VPC)-Endpunkte mit S3-Bucket-Richtlinien verwenden, um den Zugriff auf bestimmte VPC-Endpunkte zu beschränken. Weitere Informationen finden Sie unter Steuern des Zugriffs von VPC-Endpunkten mit Bucket-Richtlinien im Amazon S3-Benutzerhandbuch
- Um vertrauenswürdigen Entitäten außerhalb Ihres Kontos vorübergehend den Zugriff auf Ihre S3-Objekte zu gewähren, können Sie über S3 eine vorsignierte URL erstellen. Dieser Zugriff wird mit Ihren Konto-Anmeldeinformationen erstellt und kann je nach den verwendeten Anmeldeinformationen 6 Stunden bis 7 Tage dauern. Weitere Informationen finden Sie unter Verwenden vorsignierter URLs zum Herunterladen und Hochladen von Objekten im Amazon S3-Benutzerhandbuch.

- Für Anwendungsfälle, die die gemeinsame Nutzung von S3-Objekten zwischen verschiedenen Quellen erfordern, können Sie S3-Zugangspunkte verwenden, um Berechtigungssätze zu erstellen, die den Zugriff nur auf diejenigen innerhalb Ihres privaten Netzwerks beschränken. Weitere Informationen finden Sie unter Verwaltung des Zugriffs auf gemeinsam genutzte Datensätze mit Access Points im Amazon S3-Benutzerhandbuch.
- Um anderen AWS Konten sicher Zugriff auf Ihre S3-Ressourcen zu gewähren, können Sie eine Zugriffskontrollliste (ACL) verwenden. Weitere Informationen finden Sie im Überblick über die Zugriffskontrollliste (ACL) im Amazon S3-Benutzerhandbuch.

Weitere Informationen zu den S3-Sicherheitsoptionen finden Sie unter Bewährte Sicherheitsmethoden für Amazon S3 im Amazon S3-Benutzerhandbuch.

Behebung eines potenziell bösartigen S3-Objekts

Wenn es GuardDuty generiert wirdSuchtyp „Malware-Schutz für S3“, bedeutet dies, dass ein neu hochgeladenes Objekt in Ihrem Amazon S3-Bucket Malware enthält. Der Ressourcentyp ist ein S3-Objekt.

Verwenden Sie die folgenden empfohlenen Schritte, um das generierte Ergebnis möglicherweise zu korrigieren:

1. Identifizieren Sie das potenziell bösartige S3-Objekt, indem Sie das mit dem Ergebnis S3ObjectDetails verknüpfte Objekt überprüfen.
2. Isolieren Sie das betroffene S3-Objekt. Wenn Sie zum Zeitpunkt der Aktivierung von Malware Protection for S3 für den zugehörigen Amazon S3-Bucket das Tagging aktiviert hatten, GuardDuty müssen Sie diesem Objekt ein bösartiges Tag zugewiesen haben. Verwenden Sie die tagbasierte Zugriffskontrolle (TBAC), um den Zugriff auf dieses S3-Objekt einzuschränken. Weitere Informationen finden Sie unter Verwenden der tagbasierten Zugriffskontrolle (TBAC).

   Wenn Sie dieses Objekt nicht mehr benötigen, können Sie es alternativ auch löschen oder in einen isolierten S3-Bucket verschieben. Informationen zu Überlegungen beim Löschen eines S3-Objekts finden Sie unter Löschen von Objekten im Amazon S3-Benutzerhandbuch.

Behebung eines potenziell kompromittierten EBS-Snapshots

Wann generiert ein! GuardDuty Execution:EC2/MaliciousFile Der Typ des Snapshot-Findens gibt an, dass in einem Amazon EBS-Snapshot Malware erkannt wurde. Führen Sie die folgenden Schritte aus, um den potenziell kompromittierten Snapshot zu beheben:

1. Identifizieren Sie den potenziell gefährdeten Snapshot

    1. Identifizieren Sie den potenziell kompromittierten Snapshot. Bei der GuardDuty Suche nach einem EBS-Snapshot werden die betroffene Snapshot-ID, der Amazon-Ressourcenname (ARN) und die zugehörigen Malware-Scan-Details in den Funddetails aufgeführt.
    2. Überprüfen Sie die Details des Wiederherstellungspunkts mit dem folgenden Befehl:

    ```
    aws backup describe-recovery-point –backup-vault-name 021345abcdef6789 –recovery-point-arn "arn:aws:ec2:us-east-1::snapshot/snap-abcdef01234567890"
    ```

2. Beschränken Sie den Zugriff auf den kompromittierten Snapshot

    Überprüfen und ändern Sie die Richtlinien für den Zugriff auf den Backup-Tresor, um den Zugriff auf den Recovery Point einzuschränken und alle automatisierten Wiederherstellungsaufträge auszusetzen, die diesen Snapshot möglicherweise verwenden.

    1. Überprüfen Sie die aktuellen Freigabeberechtigungen:

    ```
    aws ec2 describe-snapshot-attribute --snapshot-id snap-abcdef01234567890 --attribute createVolumePermission
    ```

    2. Bestimmte Kontozugriffe entfernen:

    ```
    aws ec2 modify-snapshot-attribute --snapshot-id snap-abcdef01234567890 --attribute createVolumePermission --operation-type remove --user-ids 111122223333
    ```

    3. Weitere CLI-Optionen finden Sie in der CLI-Dokumentation zu modify-snapshot-attribute.

3. Ergreifen Sie Abhilfemaßnahmen

    - Bevor Sie mit dem Löschen fortfahren, stellen Sie sicher, dass Sie alle Abhängigkeiten identifiziert haben und bei Bedarf über geeignete Backups verfügen.

Behebung eines potenziell kompromittierten EC2-AMI

Wann generiert ein! GuardDuty Execution:EC2/MaliciousFile AMI-Findetyp. Er weist darauf hin, dass Malware in einem Amazon Machine Image (AMI) erkannt wurde. Führen Sie die folgenden Schritte durch, um das potenziell kompromittierte AMI zu beheben:

1. Identifizieren Sie das potenziell gefährdete AMI
    1. Bei einer GuardDuty Suche nach AMIs werden die betroffene AMI-ID, ihr Amazon-Ressourcenname (ARN) und die zugehörigen Malware-Scandetails in den Funddetails aufgeführt.
    2. Überprüfen Sie das AMI-Quellbild:

        ```
        aws ec2 describe-images --image-ids ami-021345abcdef6789
        ```

2. Beschränken Sie den Zugriff auf die gefährdeten Ressourcen
    1. Überprüfen und ändern Sie die Richtlinien für den Zugriff auf den Backup-Tresor, um den Zugriff auf den Recovery-Punkt einzuschränken und alle automatisierten Wiederherstellungsaufträge auszusetzen, die diesen Recovery-Punkt möglicherweise verwenden.
    2. Entfernen Sie die Berechtigungen aus den AMI-Quellberechtigungen

        Sehen Sie sich zuerst die vorhandenen Berechtigungen an:

        ```
        aws ec2 describe-image-attribute --image-id ami-abcdef01234567890 --attribute
         launchPermission
        ```

        Dann entferne einzelne Berechtigungen:

        ```
        aws ec2 modify-image-attribute --image-id ami-abcdef01234567890 --launch-
        permission '{"Remove":[{"UserId":"111122223333"}]}'
        ```

        Weitere CLI-Optionen finden Sie unter Ein AMI mit bestimmten Konten teilen — Amazon Elastic Compute Cloud
    3. Wenn es sich bei der Quelle um eine EC2-Instance handelt, siehe: Behebung einer potenziell kompromittierten Amazon EC2-Instance.
3. Ergreifen Sie Abhilfemaßnahmen

- Bevor Sie mit dem Löschen fortfahren, stellen Sie sicher, dass Sie alle Abhängigkeiten identifiziert haben und bei Bedarf über geeignete Backups verfügen.

Behebung eines potenziell kompromittierten EC2-Wiederherstellungspunkts

Wann generiert ein! GuardDuty Execution:EC2/MaliciousFile RecoveryPoint Wenn der Typ gefunden wird, bedeutet dies, dass in einer EC2 Recovery Point Backup-Ressource Schadsoftware entdeckt wurde. Führen Sie die folgenden Schritte durch, um den potenziell gefährdeten Recovery-Punkt zu reparieren:

1. Identifizieren Sie den potenziell gefährdeten EC2-Wiederherstellungspunkt

    1. Bei einer GuardDuty Suche nach EC2 Recovery Point werden der Amazon-Ressourcenname (ARN) und die zugehörigen Malware-Scandetails in den Funddetails aufgeführt:

        ```
        aws backup describe-recovery-point --backup-vault-name 021345abcdef6789
         --recovery-point-arn "arn:aws:backup:us-east-1:111122223333:recovery-
        point:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
        ```

    2. Überprüfen Sie die Wiederherstellungsdetails, um nach dem Quellbild zu suchen:

        ```
        aws backup get-recovery-point-restore-metadata --backup-vault-
        name 021345abcdef6789 --recovery-point-arn "arn:aws:backup:us-
        east-1:111122223333:recovery-point:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
        ```

2. Beschränken Sie den Zugriff auf die gefährdeten Ressourcen

    - Überprüfen und ändern Sie die Richtlinien für den Zugriff auf den Backup-Tresor, um den Zugriff auf den Recovery-Punkt einzuschränken und alle automatisierten Wiederherstellungsaufträge auszusetzen, die diesen Recovery-Punkt möglicherweise verwenden. Wenn Ihre Umgebung Ressourcen-Tagging verwendet, kennzeichnen Sie den Recovery-Punkt entsprechend, um anzuzeigen, dass er gerade untersucht wird, und erwägen Sie gegebenenfalls, geplante Backups zu unterbrechen.

      Beispiel:

```
aws backup tag-resource --–resource-arn arn:aws:backup:us-
east-1:111122223333:recovery-point:a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111 --–tags Investigation=Malware,DoNotDelete=True
```

3. Ergreifen Sie Abhilfemaßnahmen

   - Bevor Sie mit dem Löschen fortfahren, stellen Sie sicher, dass Sie alle Abhängigkeiten identifiziert haben und bei Bedarf über geeignete Backups verfügen.

Behebung eines potenziell kompromittierten S3-Wiederherstellungspunkts

Wann GuardDuty generiert ein! Execution:S3/MaliciousFile RecoveryPoint Wenn der Typ gefunden wird, bedeutet dies, dass in einer S3 Recovery Point Backup-Ressource Malware entdeckt wurde. Gehen Sie wie folgt vor, um den potenziell kompromittierten Wiederherstellungspunkt zu reparieren:

1. Identifizieren Sie den potenziell gefährdeten S3-Wiederherstellungspunkt

   1. Bei der GuardDuty Suche nach S3-Wiederherstellungspunkten werden der ARN des betroffenen Wiederherstellungspunkts, der Name des Backup-Tresors und die zugehörigen Malware-Scandetails in den Erkennungsdetails aufgeführt.
   2. Überprüfen Sie die Details des Wiederherstellungspunkts:

      ```
      aws backup describe-recovery-point --backup-vault-name 021345abcdef6789
       --recovery-point-arn arn:aws:backup:us-east-1:123456789012:recovery-
      point:abcdef01234567890
      ```

2. Beschränken Sie den Zugriff auf die gefährdeten Ressourcen

   - Überprüfen und ändern Sie die Richtlinien für den Zugriff auf den Backup-Tresor, um den Zugriff auf den Recovery-Punkt einzuschränken und alle automatisierten Wiederherstellungsaufträge auszusetzen, die diesen Recovery-Punkt möglicherweise verwenden. Wenn Ihre Umgebung Ressourcen-Tagging verwendet, kennzeichnen Sie den Recovery-Punkt entsprechend, um anzuzeigen, dass er gerade untersucht wird, und erwägen Sie gegebenenfalls, geplante Backups zu unterbrechen.

     Beispiel:

```
aws backup tag-resource –resource-arn arn:aws:backup:us-
east-1:111122223333:recovery-point:abcdef01234567890 –
tags Investigation=Malware,DoNotDelete=True
```

Weitere Informationen finden Sie unter: tag-resource CLI-Befehlsreferenz

3. Ergreifen Sie Abhilfemaßnahmen

   - Bevor Sie mit dem Löschen fortfahren, stellen Sie sicher, dass Sie alle Abhängigkeiten identifiziert haben und bei Bedarf über geeignete Backups verfügen.

Behebung eines potenziell kompromittierten ECS-Clusters

Ein potenziell kompromittierter ECS-Cluster weist darauf hin, dass in Ihrer Amazon ECS-Umgebung verdächtige oder böswillige Aktivitäten erkannt wurden. Dazu können unbefugter Zugriff, die Ausführung von Malware oder anderes bösartiges Verhalten gehören, das Ihre Container-Workloads gefährdet.

Folgen Sie diesen Schritten, um ein potenziell kompromittiertes Amazon ECS-Cluster zu beheben:

1. Identifizieren Sie den potenziell gefährdeten ECS-Cluster und die erkannte Bedrohung (Ergebnisse)

   Die Details zum betroffenen ECS-Cluster sind im Bereich mit den GuardDuty Funddetails aufgeführt.

2. Bewerten Sie die Quelle von threat/malware

   Suchen Sie nach Malware in Container-Images. Wenn Malware erkannt wird, überprüfen Sie das verwendete Container-Image. Wird verwendet ListTasks, um alle anderen laufenden Aufgaben zu identifizieren, die dasselbe potenziell gefährdete Image verwenden.

3. Isolieren Sie betroffene Aufgaben

   Stoppen Sie die Bedrohung, indem Sie den gesamten Netzwerkverkehr (sowohl eingehend als auch ausgehend) zu den betroffenen Aufgaben blockieren. Diese Netzwerkisolierung hilft, laufende Angriffe zu verhindern, indem alle Verbindungen zu der gefährdeten Aufgabe unterbrochen werden.

Hinweis: Wenn Sie feststellen, dass dieser Befund durch expected/legitimate Aktivitäten in Ihrer Umgebung ausgelöst wurde, können Sie eine Unterdrückungsregel einrichten, um zu verhindern, dass ähnliche Ergebnisse angezeigt werden. Weitere Informationen finden Sie unter Unterdrückungsregeln in GuardDuty.

Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten

Bei der GuardDuty Generierung wird darauf hingewiesenIAM-Erkenntnistypen, dass Ihre AWS Anmeldeinformationen kompromittiert wurden. Der potenziell gefährdete Ressourcentyp ist. AccessKey

Gehen Sie wie folgt vor, um potenziell kompromittierte Anmeldeinformationen in Ihrer AWS Umgebung zu beheben:

1. Identifizieren Sie die potenziell gefährdete IAM-Entität und den verwendeten API-Aufruf.

   Der verwendete API-Aufruf wird in den Ergebnisdetails als `API` aufgelistet. Die IAM-Entität (entweder eine IAM-Rolle oder ein IAM-Benutzer) und ihre identifizierenden Informationen werden im Abschnitt „Ressource“ der Ergebnisdetails aufgeführt. Der Typ der beteiligten IAM-Entität kann anhand des Feldes Benutzertyp bestimmt werden. Der Name der IAM-Entität befindet sich im Feld Benutzername. Der Typ von IAM-Entität, der an einem Ergebnis beteiligt ist, kann auch anhand der verwendeten Zugriffsschlüssel-ID bestimmt werden.

   Für Schlüssel, die mit `AKIA` beginnen:

   Bei dieser Art von Schlüssel handelt es sich um langfristige, vom Kunden verwaltete Anmeldeinformationen, die einem IAM-Benutzer oder Root-Benutzer des AWS-Kontos zugeordnet sind. Weitere Informationen zum Verwalten von Zugriffsschlüsseln für IAM-Benutzer finden Sie unter Verwalten von Zugriffsschlüsseln für IAM-Benutzer.

   Für Schlüssel, die mit `ASIA` beginnen:

   Bei dieser Art von Schlüssel handelt es sich um kurzfristige temporäre Anmeldeinformationen, die von AWS -Security-Token-Service generiert werden. Diese Schlüssel existieren nur für kurze Zeit und können in der AWS Managementkonsole nicht angezeigt oder verwaltet werden. IAM-Rollen verwenden immer AWS STS Anmeldeinformationen, sie können aber auch für IAM-Benutzer generiert werden. Weitere Informationen AWS STS finden Sie unter IAM: Temporäre Sicherheitsanmeldeinformationen.

Wenn eine Rolle verwendet wurde, enthält das Feld Benutzername den Namen der verwendeten Rolle. Sie können anhand des `sessionIssuer` Elements des CloudTrail Protokolleintrags feststellen, wie der Schlüssel angefordert wurde. Weitere Informationen finden Sie unter IAM und Informationen unter. AWS CloudTrailAWS STS CloudTrail

2. Überprüfen Sie die Berechtigungen für die IAM-Entität.

   Öffnen Sie die IAM-Konsole. Wählen Sie je nach Typ der verwendeten Entität die Registerkarte Benutzer oder Rollen und suchen Sie die betroffene Entität, indem Sie den identifizierten Namen in das Suchfeld eingeben. Überprüfen Sie über die Registerkarten Berechtigung und Access Advisor effektive Berechtigungen für diese Entität.

3. Bestimmen Sie, ob die Anmeldeinformationen der IAM-Entität rechtmäßig verwendet wurden.

   Wenden Sie sich an den Benutzer der Anmeldeinformationen, um festzustellen, ob die Aktivität beabsichtigt war.

   Ermitteln Sie beispielsweise, ob der Benutzer die Anmeldeinformationen zu Folgendem verwendet hat:

   - Hat den API-Vorgang aufgerufen, der im GuardDuty Ergebnis aufgeführt wurde
   - Zum Aufrufen der API-Operation zu dem im GuardDuty-Ergebnis angegebenen Zeitpunkt
   - Zum Aufrufen der API-Operation von der im GuardDuty -Ergebnis angegebenen IP-Adresse aus

Wenn es sich bei dieser Aktivität um eine legitime Verwendung der AWS Anmeldeinformationen handelt, können Sie das GuardDuty Ergebnis ignorieren. In der https://console.aws.amazon.com/guardduty/ Konsole können Sie Regeln einrichten, um einzelne Ergebnisse vollständig zu unterdrücken, sodass sie nicht mehr angezeigt werden. Weitere Informationen finden Sie unter Unterdrückungsregeln in GuardDuty.

Wenn Sie nicht bestätigen können, ob es sich bei dieser Aktivität um eine legitime Nutzung handelt, könnte dies das Ergebnis einer Kompromittierung des jeweiligen Zugriffsschlüssels sein — der Anmeldeinformationen des IAM-Benutzers oder möglicherweise des gesamten. AWS-Konto Wenn Sie den Verdacht haben, dass Ihre Anmeldeinformationen missbraucht wurden, überprüfen Sie die Informationen unter Mein AWS-Konto könnte gefährdet sein, um das Problem zu beheben.

Behebung eines potenziell kompromittierten Standalone-Containers

Wenn Suchtypen GuardDuty generiert werden, die auf einen potenziell kompromittierten Container hinweisen, lautet Ihr Ressourcentyp Container. Wenn das Verhalten, das den Befund verursacht hat, in Ihrer Umgebung erwartet wurde, sollten Sie die Verwendung Unterdrückungsregeln in Betracht ziehen.

Gehen Sie wie folgt vor, um potenziell kompromittierte Anmeldeinformationen in Ihrer AWS Umgebung zu beheben:

1. Isolieren Sie den potenziell gefährdeten Container

   Die folgenden Schritte helfen Ihnen dabei, den potenziell schädlichen Container-Workload zu identifizieren:

   - Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
   - Wählen Sie auf der Seite Ergebnisse das entsprechende Ergebnis aus, um den Ergebnisbereich anzuzeigen.
   - Im Erkenntnisfenster können Sie im Abschnitt Betroffene Ressource die ID und den Namen des Containers einsehen.

   Isolieren Sie diesen Container von anderen Container-Workloads.
2. Halten Sie den Container an

   Unterbrechen Sie alle Prozesse in Ihrem Container.

   Informationen zum Einfrieren Ihres Containers finden Sie unter Einen Container anhalten.

   Stoppen Sie den Container.

   Wenn der obige Schritt fehlschlägt und der Container nicht angehalten wird, beenden Sie die Ausführung des Containers. Wenn Sie die Snapshot-Beibehaltung Funktion aktiviert haben, GuardDuty werden die Snapshots Ihrer EBS-Volumes, die Malware enthalten, beibehalten.

   Informationen zum Stoppen des Containers finden Sie unter Stoppen eines Containers.
3. Prüfen Sie das Vorhandensein von Malware

   Prüfen Sie, ob sich die entdeckte Malware im Image des Containers befand.

Wenn der Zugriff autorisiert wurde, können Sie die Erkenntnis ignorieren. In der https://console.aws.amazon.com/guardduty/ Konsole können Sie Regeln einrichten, um einzelne Ergebnisse vollständig zu unterdrücken, sodass sie nicht mehr angezeigt werden. In der GuardDuty Konsole können Sie Regeln einrichten, um einzelne Ergebnisse vollständig zu unterdrücken, sodass sie nicht mehr angezeigt werden. Weitere Informationen finden Sie unter Unterdrückungsregeln in GuardDuty.

Behebung der EKS-Schutzfeststellungen

Amazon GuardDuty generiert Ergebnisse, die auf potenzielle Kubernetes-Sicherheitsprobleme hinweisen, wenn EKS Protection für Ihr Konto aktiviert ist. Weitere Informationen finden Sie unter EKS-Schutz. In den folgenden Abschnitten werden die empfohlenen Schritte zur Behebung für alle Szenarien beschrieben. Spezifische Behebungsmaßnahmen werden im Eintrag für diesen spezifischen Erkenntnistyp beschrieben. Sie können auf die vollständigen Informationen zu einem Erkenntnistyp zugreifen, indem Sie ihn aus der Tabelle für aktive Erkenntnistypen auswählen.

Wenn einer der EKS-Protection-Erkennungstypen erwartungsgemäß generiert wurde, können Sie erwägen, ihn hinzuzufügen, um zukünftige Warnmeldungen Unterdrückungsregeln in GuardDuty zu vermeiden.

Verschiedene Arten von Angriffen und Konfigurationsproblemen können zu Ergebnissen von GuardDuty EKS Protection führen. Dieses Handbuch hilft Ihnen dabei, die Hauptursachen von GuardDuty Ergebnissen in Ihrem Cluster zu identifizieren, und enthält geeignete Anleitungen zur Problembehebung. Im Folgenden sind die Hauptursachen aufgeführt, die zu den Ergebnissen von GuardDuty Kubernetes geführt haben:

- Mögliche Konfigurationsprobleme
- Behebung potenziell gefährdeter Kubernetes-Benutzer
- Behebung potenziell kompromittierter Kubernetes-Pods
- Behebung potenziell kompromittierter Kubernetes-Knoten
- Behebung potenziell kompromittierter Container-Images

> **Note**
>
> Vor Kubernetes-Version 1.14 war die `system:unauthenticated` Gruppe standardmäßig mit und verknüpft. `system:discovery` `system:basic-user` ClusterRoles Dies

könnte unbeabsichtigten Zugriff durch anonyme Benutzer ermöglichen. Durch Cluster-Updates werden diese Berechtigungen nicht aufgehoben. Das bedeutet, dass diese Berechtigungen auch dann noch gültig sind, wenn Sie Ihren Cluster auf Version 1.14 oder höher aktualisiert haben. Wir empfehlen, dass Sie die Zuordnung dieser Berechtigungen zu der `system:unauthenticated`-Gruppe aufheben.
Weitere Informationen zum Entfernen dieser Berechtigungen finden Sie unter Sichern von Amazon EKS-Clustern mit bewährten Methoden im Amazon EKS-Benutzerhandbuch.

Mögliche Konfigurationsprobleme

Wenn eine Erkenntnis auf ein Konfigurationsproblem hindeutet, finden Sie im Abschnitt zur Behebung dieses Fehlers Anleitungen zur Lösung dieses speziellen Problems. Weitere Informationen finden Sie unter den folgenden Erkenntnistypen, die auf Konfigurationsprobleme hinweisen:

- Policy:Kubernetes/AnonymousAccessGranted
- Policy:Kubernetes/ExposedDashboard
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount
- Policy:Kubernetes/KubeflowDashboardExposed
- Jeder Befund, der endet in SuccessfulAnonymousAccess

Behebung potenziell gefährdeter Kubernetes-Benutzer

Ein GuardDuty Ergebnis kann auf einen kompromittierten Kubernetes-Benutzer hinweisen, wenn ein in dem Ergebnis identifizierter Benutzer eine unerwartete API-Aktion ausgeführt hat. Sie können den Benutzer im Bereich Kubernetes-Benutzerdetails im Erkenntnisfenster der Konsole oder in der `resource.kubernetesDetails.kubernetesUserDetails` der JSON-Datei mit den Erkenntnissen identifizieren. Zu diesen Benutzerdetails gehören `user name`, `uid` und die Kubernetes-Gruppen, zu denen der Benutzer gehört.

Wenn der Benutzer mit einer IAM-Entität auf den Workload zugegriffen hat, können Sie den `Access Key details`-Abschnitt verwenden, um die Details einer IAM-Rolle oder eines IAM-Benutzers zu identifizieren. Sehen Sie sich die folgenden Benutzertypen und deren Anleitungen zur Problembehebung an.

> **Note**
>
> Sie können Amazon Detective verwenden, um die in der Erkenntnis identifizierte IAM-Rolle oder den IAM-Benutzer genauer zu untersuchen. Wählen Sie „In Detective untersuchen“, während Sie sich die Befunddetails in der GuardDuty Konsole ansehen. Wählen Sie dann den AWS Benutzer oder die Rolle aus den aufgelisteten Objekten aus, um den Vorgang in Detective zu untersuchen.

Built-in Kubernetes-Admin — Der Standardbenutzer, der von Amazon EKS der IAM-Identität zugewiesen wurde, die den Cluster erstellt hat. Dieser Benutzertyp wird durch den Benutzernamen identifiziert `kubernetes-admin`.

Wie Sie einem integrierten Kubernetes-Administrator den Zugriff entziehen:

- Identifizieren Sie den `userType` aus dem `Access Key details`-Abschnitt.
  - Wenn der `userType` Rolle ist und die Rolle zu einer EC2-Instance-Rolle gehört:
    - Identifizieren Sie diese Instance und folgen Sie dann den Anweisungen unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.
  - Wenn es sich bei `userType` um einen Benutzer handelt oder um eine Rolle, die von einem Benutzer übernommen wurde:
    1. Rotieren Sie den Zugriffsschlüssel dieses Benutzers.
    2. Rotieren Sie alle Geheimnisse, auf die der Benutzer Zugriff hatte.
    3. Weitere Informationen finden Sie in den Informationen unter Mein ist AWS-Konto möglicherweise kompromittiert.

OIDC-authentifizierter Benutzer – Ein Benutzer, dem der Zugriff über einen OIDC-Anbieter gewährt wurde. In der Regel hat ein OIDC-Benutzer eine E-Mail-Adresse als Benutzernamen. Sie können mit den folgenden Befehl überprüfen, ob Ihr Cluster OIDC verwendet: `aws eks list-identity-provider-configs --cluster-name` *`your-cluster-name`*

Um einem OIDC-authentifizierten Benutzer den Zugriff zu entziehen:

1. Rotieren Sie die Anmeldeinformationen dieses Benutzers im OIDC-Anbieter.
2. Rotieren Sie alle Geheimnisse, auf die der Benutzer Zugriff hatte.

AWS ConfigMap -Auth-definierter Benutzer — Ein IAM-Benutzer, dem der Zugriff über ein -auth gewährt wurde. AWS ConfigMap Weitere Informationen finden Sie im Amazon EKS-Benutzerhandbuch unter Benutzer oder IAM-Rollen für Ihren Cluster https://docs.aws.amazon.com/eks/latest/userguide/add-user-role.html verwalten. Sie können ihre Berechtigungen überprüfen, indem Sie den folgenden Befehl verwenden: `kubectl edit configmaps aws-auth --namespace kube-system`

So entziehen Sie einem AWS ConfigMap Benutzer den Zugriff:

1. Verwenden Sie den folgenden Befehl, um das zu öffnen ConfigMap.

```
kubectl edit configmaps aws-auth --namespace kube-system
```

2. Identifizieren Sie die Rolle oder den Benutzereintrag im Abschnitt MapRoles oder MapUsers mit demselben Benutzernamen wie dem, der im Abschnitt mit den Kubernetes-Benutzerdetails Ihres Ergebnisses angegeben wurde. GuardDuty Sehen Sie sich das folgende Beispiel an, in dem der Admin-Benutzer in einer Erkenntnis identifiziert wurde.

```
apiVersion: v1
data:
  mapRoles: |
    - rolearn: arn:aws:iam::444455556666:role/eksctl-my-cluster-nodegroup-
standard-wo-NodeInstanceRole-1WP3NUE3O6UCF
      user name: system:node:EC2_PrivateDNSName
      groups:
        - system:bootstrappers
        - system:nodes
  mapUsers: |
    - userarn: arn:aws:iam::123456789012:user/admin
      username: admin
      groups:
        - system:masters
    - userarn: arn:aws:iam::111122223333:user/ops-user
      username: ops-user
      groups:
        - system:masters
```

3. Entfernen Sie diesen Benutzer aus dem. ConfigMap Sehen Sie sich das folgende Beispiel an, in dem der Admin-Benutzer entfernt wurde.

```
apiVersion: v1
data:
```

```
  mapRoles: |
    - rolearn: arn:aws:iam::111122223333:role/eksctl-my-cluster-nodegroup-
standard-wo-NodeInstanceRole-1WP3NUE3O6UCF
      username: system:node:{{EC2PrivateDNSName}}
      groups:
        - system:bootstrappers
        - system:nodes
  mapUsers: |
    - userarn: arn:aws:iam::111122223333:user/ops-user
      username: ops-user
      groups:
        - system:masters
```

4. Wenn es sich bei `userType` um einen Benutzer handelt oder um eine Rolle, die von einem Benutzer übernommen wurde:
   a. Rotieren Sie den Zugriffsschlüssel dieses Benutzers.
   b. Rotieren Sie alle Geheimnisse, auf die der Benutzer Zugriff hatte.
   c. Weitere Informationen finden Sie unter Mein AWS Konto ist möglicherweise kompromittiert.

Wenn die Erkenntnis keinen `resource.accessKeyDetails`-Abschnitt enthält, handelt es sich bei dem Benutzer um ein Kubernetes-Servicekonto.

Servicekonto – Das Servicekonto stellt eine Identität für Pods bereit und kann anhand eines Benutzernamens mit dem folgenden Format identifiziert werden: `system:serviceaccount:`*`namespace`*`:`*`service_account_name`*.

Um den Zugriff auf ein Servicekonto zu widerrufen:

1. Rotieren Sie die Anmeldeinformationen für das Servicekonto.
2. Lesen Sie die Hinweise zur Pod-Kompromittierung im folgenden Abschnitt.

Behebung potenziell kompromittierter Kubernetes-Pods

Wenn in dem `resource.kubernetesDetails.kubernetesWorkloadDetails` Abschnitt Details zu einem Pod oder einer Workload-Ressource GuardDuty angegeben sind, wurde dieser Pod oder diese Workload-Ressource potenziell gefährdet. Ein GuardDuty Ergebnis kann darauf hindeuten, dass ein einzelner Pod kompromittiert wurde oder dass mehrere Pods durch eine übergeordnete Ressource kompromittiert wurden. In den folgenden Kompromissszenarien finden Sie Anleitungen zur Identifizierung des oder der Pods, die kompromittiert wurden.

Kompromittierung einzelner Pods

Wenn es sich bei dem `type`-Feld innerhalb des `resource.kubernetesDetails.kubernetesWorkloadDetails`-Abschnitts um Pods handelt, identifiziert die Erkenntnis einzelne Pods. Das Namensfeld ist der `name` der Pods und das `namespace`-Feld ist sein Namespace.

Informationen zur Identifizierung des Worker-Knotens, auf dem die Pods ausgeführt werden, finden Sie im Amazon EKS-Handbuch mit den Best Practices unter Identifizieren der fehlerhaften Pods und des Worker-Knotens.

Pods wurden über die Workload-Ressource kompromittiert

Wenn das `type`-Feld innerhalb des `resource.kubernetesDetails.kubernetesWorkloadDetails`-Abschnitts eine Workload-Ressource identifiziert, z. B. eine `Deployment`, ist es wahrscheinlich, dass alle Pods innerhalb dieser Workload-Ressource kompromittiert wurden.

Informationen zur Identifizierung aller Pods der Workload-Ressource und der Knoten, auf denen sie ausgeführt werden, finden Sie im Amazon EKS-Handbuch mit den Best Practices unter Identifizieren der fehlerhaften Pods und Worker-Knoten anhand des Workload-Namens.

Pods wurden über das Servicekonto kompromittiert

Wenn GuardDuty bei einer Entdeckung im `resource.kubernetesDetails.kubernetesUserDetails` Abschnitt ein Servicekonto identifiziert wird, ist es wahrscheinlich, dass Pods, die das identifizierte Dienstkonto verwenden, gefährdet sind. Der durch eine Erkenntnis gemeldete Benutzername ist ein Servicekonto, wenn er das folgende Format hat: `system:serviceaccount:`*`namespace`*`:`*`service_account_name`*.

Informationen zur Identifizierung aller Pods, die das Dienstkonto verwenden, und der Knoten, auf denen sie ausgeführt werden, finden Sie im Amazon EKS-Handbuch mit den Best Practices unter Identifizieren der problematischen Pods und Worker-Nodes anhand des Dienstkontonamens.

Nachdem Sie alle gefährdeten Pods und die Knoten, auf denen sie ausgeführt werden, identifiziert haben, finden Sie im Amazon EKS Best Practices-Leitfaden unter Isolieren Sie den Pod, indem Sie eine Netzwerkrichtlinie erstellen, die den gesamten ein- und ausgehenden Datenverkehr zum Pod ablehnt.

So beheben Sie einen potenziell kompromittierten Pod:

1. Identifizieren Sie die Schwachstelle, durch die die Pods gefährdet wurden.
2. Implementieren Sie das Update für diese Schwachstelle und starten Sie neue Ersatz-Pods.
3. Löschen Sie die anfälligen Pods.

   Weitere Informationen finden Sie im Amazon EKS-Leitfaden zu Best Practices unter Redeploy Compromitted Pod oder Workload-Ressource.

Wenn dem Worker-Knoten eine IAM-Rolle zugewiesen wurde, die es Pods ermöglicht, auf andere AWS Ressourcen zuzugreifen, entfernen Sie diese Rollen aus der Instance, um weiteren Schaden durch den Angriff zu verhindern. Wenn dem Pod eine IAM-Rolle zugewiesen wurde, sollten Sie ebenfalls prüfen, ob Sie die IAM-Richtlinien sicher aus der Rolle entfernen können, ohne andere Workloads zu beeinträchtigen.

Behebung potenziell kompromittierter Container-Images

Wenn ein GuardDuty Befund darauf hindeutet, dass der Pod kompromittiert wurde, könnte das zum Starten des Pods verwendete Image potenziell bösartig oder kompromittiert sein. GuardDuty Die Ergebnisse identifizieren das Container-Image innerhalb des `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.image` Felds. Sie können feststellen, ob das Image bösartig ist, indem Sie es auf Malware scannen.

So beheben Sie ein potenziell kompromittiertes Container-Image:

1. Beenden Sie sofort die Verwendung des Images und entfernen Sie es aus Ihrem Image-Repository.
2. Identifizieren Sie alle Pods, die das potenziell kompromittierte Image verwenden.

   Weitere Informationen finden Sie im Amazon EKS Best Practices Guide unter Identifizieren von Pods mit anfälligen oder gefährdeten Images und Worker-Knoten.
3. Isolieren Sie die potenziell gefährdeten Pods, rotieren Sie die Anmeldeinformationen und sammeln Sie Daten für die Analyse. Weitere Informationen finden Sie im Amazon EKS Best Practices Guide unter Isolieren Sie den Pod, indem Sie eine Netzwerkrichtlinie erstellen, die den gesamten ein- und ausgehenden Datenverkehr zum Pod ablehnt.
4. Löschen Sie alle Pods, die das potenziell kompromittierte Image verwenden.

Behebung potenziell kompromittierter Kubernetes-Knoten

Ein GuardDuty Ergebnis kann auf eine Node-Kompromittierung hinweisen, wenn der im Ergebnis identifizierte Benutzer eine Node-Identität repräsentiert oder wenn das Ergebnis auf die Verwendung eines privilegierten Containers hindeutet.

Die Benutzeridentität ist ein Worker-Knoten, wenn das Feld für den Benutzernamen das folgende Format hat: `system:node:node name`. Beispiel, `system:node:ip-192-168-3-201.ec2.internal`. Dies weist darauf hin, dass der Angreifer Zugriff auf den Knoten erhalten hat und die Anmeldeinformationen des Knotens verwendet, um mit dem Kubernetes-API-Endpunkt zu kommunizieren.

Eine Erkenntnis weist auf die Verwendung eines privilegierten Containers hin, wenn für einen oder mehrere der in der Erkenntnis aufgelisteten Container das Erkenntnisfeld `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.securityContext.` auf `True` gesetzt ist.

Gehen Sie wie folgt vor, um einen potenziell kompromittierten Knoten zu beheben:

1. Isolieren Sie den Pod, wechseln Sie seine Anmeldeinformationen und sammeln Sie Daten für die forensische Analyse.

   Weitere Informationen finden Sie im Amazon EKS Best Practices Guide unter Isolieren Sie den Pod, indem Sie eine Netzwerkrichtlinie erstellen, die den gesamten ein- und ausgehenden Datenverkehr zum Pod ablehnt.
2. Identifizieren Sie die Dienstkonten, die von allen Pods verwendet werden, die auf dem potenziell gefährdeten Knoten ausgeführt werden. Überprüfen Sie ihre Berechtigungen und rotieren Sie die Servicekonten bei Bedarf.
3. Beenden Sie den potenziell gefährdeten Knoten.

Korrigieren von Erkenntnissen der Laufzeitüberwachung

Wenn Sie Runtime Monitoring für Ihr Konto aktivieren, generiert Amazon GuardDuty möglicherweise InformationenGuardDuty Findetypen für die Laufzeitüberwachung, die auf potenzielle Sicherheitsprobleme in Ihrer AWS Umgebung hinweisen. Die potenziellen Sicherheitsprobleme deuten entweder auf eine kompromittierte Amazon EC2-Instance, einen Container-Workload, einen Amazon EKS-Cluster oder eine Reihe kompromittierter Anmeldeinformationen in Ihrer Umgebung hin. AWS Der Security Agent überwacht Laufzeitereignisse mehrerer Ressourcentypen. Um die potenziell

gefährdete Ressource zu identifizieren, sehen Sie sich den Ressourcentyp in den generierten Ergebnisdetails in der GuardDuty Konsole an. Im folgenden Abschnitt werden die empfohlenen Behebungsschritte für alle Szenarien beschrieben.

Instance

Wenn der Ressourcentyp in den Erkenntnisdetails Instance lautet, deutet dies darauf hin, dass entweder eine EC2-Instance oder ein EKS-Knoten potenziell kompromittiert ist.

- Informationen zur Behebung eines kompromittierten EKS-Knotens finden Sie unter Behebung potenziell kompromittierter Kubernetes-Knoten.
- Informationen zur Behebung einer kompromittierten EC2-Instance finden Sie unter Behebung einer potenziell kompromittierten Amazon EC2-Instance.

EKSCluster

Wenn der Ressourcentyp in den Erkenntnisdetails EKSCluster lautet, deutet dies darauf hin, dass entweder ein Pod oder ein Container in einem EKS-Cluster potenziell kompromittiert ist.

- Informationen zur Behebung eines kompromittierten Pods finden Sie unter Behebung potenziell kompromittierter Kubernetes-Pods.
- Informationen zur Behebung eines kompromittierten Container-Images finden Sie unter Behebung potenziell kompromittierter Container-Images.

ECSCluster

Wenn der Ressourcentyp in den Ergebnisdetails ecsCluster lautet, bedeutet dies, dass entweder eine ECS-Aufgabe oder ein Container innerhalb einer ECS-Aufgabe potenziell gefährdet ist.

1. Identifizieren Sie den betroffenen ECS-Cluster

   Das GuardDuty Runtime Monitoring-Ergebnis enthält die ECS-Cluster-Details im Detailbereich des Ergebnisses oder im `resource.ecsClusterDetails` Abschnitt im Ergebnis-JSON.
2. Identifizieren Sie die betroffene ECS-Aufgabe

   Das GuardDuty Runtime Monitoring-Ergebnis enthält die Details der ECS-Aufgabe im Detailbereich des Ergebnisses oder im `resource.ecsClusterDetails.taskDetails` Abschnitt im Ergebnis-JSON.

3. Isolieren Sie die betroffene Aufgabe

   Isolieren Sie die betroffene Aufgabe, indem Sie den gesamten ein- und ausgehenden Datenverkehr für die Aufgabe blockieren. Eine Regel zum Verweigern des gesamten Datenverkehrs kann dazu beitragen, einen Angriff zu stoppen, der bereits im Gange ist, indem alle Verbindungen zu der Aufgabe unterbrochen werden.
4. Korrigieren Sie die kompromittierte Aufgabe
   a. Identifizieren Sie die Sicherheitslücke, durch die die Aufgabe gefährdet wurde.
   b. Implementieren Sie den Fix für diese Sicherheitsanfälligkeit und starten Sie eine neue Ersatzaufgabe.
   c. Stoppen Sie die anfällige Aufgabe.

Container

Wenn der Ressourcentyp in den Erkenntnisdetails Container lautet, deutet dies darauf hin, dass ein alleinstehender Container potenziell kompromittiert ist.

- Informationen zur Problembehebung finden Sie unter Behebung eines potenziell kompromittierten Standalone-Containers.
- Falls die Erkenntnis für mehrere Container mit demselben Container-Image generiert wird, finden Sie weitere Informationen unter Behebung potenziell kompromittierter Container-Images.
- Wenn der Container auf den zugrunde liegenden EC2-Host zugegriffen hat, wurden die zugehörigen Instance-Anmeldeinformationen möglicherweise kompromittiert. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Bedrohungen AWS Anmeldedaten.
- Wenn ein potenziell böswilliger Akteur auf den zugrunde liegenden EKS-Knoten oder eine EC2-Instance zugegriffen hat, finden Sie unter den Registerkarten EKSCluster und Instance die empfohlenen Abhilfemaßnahmen.

Behebung kompromittierter Container-Images

Wenn ein GuardDuty Befund darauf hindeutet, dass die Aufgabe kompromittiert wurde, könnte das zum Starten der Aufgabe verwendete Image bösartig oder kompromittiert sein. GuardDuty Die Ergebnisse identifizieren das Container-Image innerhalb des `resource.ecsClusterDetails.taskDetails.containers.image` Felds. Sie können feststellen, ob das Bild schädlich ist, indem Sie es auf Malware scannen.

Um ein kompromittiertes Container-Image zu reparieren

1. Beenden Sie sofort die Verwendung des Images und entfernen Sie es aus Ihrem Image-Repository.
2. Identifizieren Sie alle Aufgaben, die dieses Image verwenden.
3. Beenden Sie alle Aufgaben, die das kompromittierte Image verwenden. Aktualisieren Sie ihre Aufgabendefinitionen, sodass sie das kompromittierte Image nicht mehr verwenden.

Behebung einer potenziell gefährdeten Datenbank

GuardDuty GeneratorenErkenntnistypen für RDS Protection, die auf ein potenziell verdächtiges und ungewöhnliches Anmeldeverhalten in Ihrem Unterstützte Datenbanken nach der Aktivierung hinweisen. RDS Protection GuardDuty Analysiert und profiliert mithilfe von RDS-Anmeldeaktivitäten Bedrohungen, indem ungewöhnliche Muster bei Anmeldeversuchen identifiziert werden.

> **Note**
>
> Sie können auf die vollständigen Informationen zu einem Erkenntnistyp zugreifen, indem Sie ihn aus der GuardDuty Typen von aktiven Ergebnissen auswählen.

Folgen Sie diesen empfohlenen Schritten, um eine potenziell gefährdete Amazon Aurora Aurora-Datenbank in Ihrer AWS Umgebung zu beheben.

Themen

- Behebung einer potenziell gefährdeten Datenbank mit erfolgreichen Anmeldeereignissen
- Behebung einer potenziell gefährdeten Datenbank mit erfolglosen Anmeldeereignissen
- Behebung potenziell kompromittierter Anmeldeinformationen
- Einschränken von Netzwerkzugriff

Behebung einer potenziell gefährdeten Datenbank mit erfolgreichen Anmeldeereignissen

Die folgenden empfohlenen Schritte können Ihnen helfen, eine potenziell gefährdete Aurora-Datenbank zu beheben, die im Zusammenhang mit erfolgreichen Anmeldeereignissen ungewöhnliches Verhalten zeigt.

1. Identifizieren Sie die betroffene Datenbank und den betroffenen Benutzer.

   Das generierte GuardDuty Ergebnis enthält den Namen der betroffenen Datenbank und die entsprechenden Benutzerdetails. Weitere Informationen finden Sie unter Erkenntnisdetails.

2. Bestätigen Sie, ob dieses Verhalten erwartet oder unerwartet ist.

   In der folgenden Liste sind mögliche Szenarien aufgeführt, die GuardDuty zur Generierung eines Ergebnisses geführt haben könnten:

   - Ein Benutzer, der sich nach Ablauf einer langen Zeit bei seiner Datenbank anmeldet.
   - Ein Benutzer, der sich gelegentlich bei seiner Datenbank anmeldet, z. B. ein Finanzanalyst, der sich vierteljährlich anmeldet.
   - Ein potenziell verdächtiger Akteur, der an einem erfolgreichen Anmeldeversuch beteiligt ist, gefährdet möglicherweise die Datenbank.

3. Beginnen Sie mit diesem Schritt, wenn das Verhalten unerwartet ist.

   1. Beschränken Sie den Datenbankzugriff

      Beschränken Sie den Datenbankzugriff für die verdächtigen Konten und die Quelle dieser Anmeldeaktivität. Weitere Informationen erhalten Sie unter Behebung potenziell kompromittierter Anmeldeinformationen und Einschränken von Netzwerkzugriff.

   2. Beurteilen Sie die Auswirkungen und stellen Sie fest, auf welche Informationen zugegriffen wurde.

      - Falls verfügbar, überprüfen Sie die Prüfungsprotokolle, um festzustellen, auf welche Informationen möglicherweise zugegriffen wurde. Weitere Informationen finden Sie unter Überwachung von Ereignissen, Protokollen und Streams in einem Amazon-Aurora-DB-Cluster im Amazon-Aurora-Benutzerhandbuch.
      - Stellen Sie fest, ob auf vertrauliche oder geschützte Informationen zugegriffen oder diese geändert wurden.

Behebung einer potenziell gefährdeten Datenbank mit erfolglosen Anmeldeereignissen

Die folgenden empfohlenen Schritte können Ihnen helfen, eine potenziell gefährdete Aurora-Datenbank zu beheben, die im Zusammenhang mit erfolglosen Anmeldeereignissen ungewöhnliches Verhalten zeigt.

1. Identifizieren Sie die betroffene Datenbank und den betroffenen Benutzer.

   Das generierte GuardDuty Ergebnis enthält den Namen der betroffenen Datenbank und die entsprechenden Benutzerdetails. Weitere Informationen finden Sie unter Erkenntnisdetails.

2. Identifizieren Sie die Quelle der fehlgeschlagenen Anmeldeversuche.

   Das generierte GuardDuty Ergebnis enthält die IP-Adresse und die ASN-Organisation (falls es sich um eine öffentliche Verbindung handelte) im Bereich „Akteur“ des Ergebnisfensters.

   Ein Autonomes System (AS) ist eine Gruppe von einem oder mehreren IP-Präfixen (Listen von IP-Adressen, auf die in einem Netzwerk zugegriffen werden kann), die von einem oder mehreren Netzwerkbetreibern betrieben werden und eine einzige, klar definierte Routing-Richtlinie einhalten. Netzbetreiber benötigen autonome Systemnummern (ASNs), um das Routing in ihren Netzwerken zu kontrollieren und Routing-Informationen mit anderen Internetdienstanbietern (ISPs) auszutauschen.

3. Bestätigen Sie, dass dieses Verhalten unerwartet ist.

   Prüfen Sie wie folgt, ob diese Aktivität einen Versuch darstellt, zusätzlichen unbefugten Zugriff auf die Datenbank zu erlangen:

   - Wenn es sich um eine interne Quelle handelt, überprüfen Sie, ob eine Anwendung falsch konfiguriert ist, und wiederholt versucht, eine Verbindung herzustellen.
   - Handelt es sich um einen externen Akteur, prüfen Sie, ob die entsprechende Datenbank öffentlich zugänglich ist oder ob sie falsch konfiguriert ist, sodass potenzielle böswillige Akteure gängige Benutzernamen mit Brute-Force-Angriffen verwenden können.

4. Beginnen Sie mit diesem Schritt, wenn das Verhalten unerwartet ist.

   1. Beschränken Sie den Datenbankzugriff

      Beschränken Sie den Datenbankzugriff für die verdächtigen Konten und die Quelle dieser Anmeldeaktivität. Weitere Informationen erhalten Sie unter Behebung potenziell kompromittierter Anmeldeinformationen und Einschränken von Netzwerkzugriff.

   2. Führen Sie eine Ursachenanalyse durch und ermitteln Sie die Schritte, die möglicherweise zu dieser Aktivität geführt haben.

      Richten Sie eine Warnung ein, um benachrichtigt zu werden, wenn eine Aktivität eine Netzwerkrichtlinie ändert und zu einem unsicheren Zustand führt. Weitere Informationen finden Sie unter Firewall-Richtlinien in AWS Network Firewall im Entwicklerhandbuch für AWS Network Firewall .

Behebung potenziell kompromittierter Anmeldeinformationen

Ein GuardDuty Ergebnis kann darauf hindeuten, dass die Benutzeranmeldedaten für eine betroffene Datenbank kompromittiert wurden, als der im Ergebnis identifizierte Benutzer einen unerwarteten Datenbankvorgang ausgeführt hat. Sie können den Benutzer im Bereich RDS-DB-Benutzerdetails im Suchfenster der Konsole oder in der `resource.rdsDbUserDetails` der JSON-Datei mit den Erkenntnissen identifizieren. Zu diesen Benutzerdetails gehören der Benutzername, die verwendete Anwendung, die abgerufene Datenbank, die SSL-Version und die Authentifizierungsmethode.

- Informationen zum Widerrufen des Zugriffs oder zum Wechseln von Passwörtern für bestimmte Benutzer, die an der Erkenntnis beteiligt sind, finden Sie unter Sicherheit mit Amazon Aurora MySQL oder Sicherheit mit Amazon Aurora PostgreSQL im Amazon-Aurora-Benutzerhandbuch.
- Wird verwendet AWS Secrets Manager , um die Geheimnisse für Amazon Relational Database Service (RDS) -Datenbanken sicher zu speichern und automatisch zu rotieren. Weitere Informationen finden Sie unter AWS Secrets Manager -Konzepte im AWS Secrets Manager -Benutzerhandbuch.
- Verwenden Sie die IAM-Datenbankauthentifizierung, um den Zugriff von Datenbankbenutzern zu verwalten, ohne dass Passwörter erforderlich sind. Weitere Informationen finden Sie unter IAM-Datenbank-Authentifizierung im Amazon Aurora-Benutzerhandbuch.

  Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Amazon Relational Database Service im Amazon-RDS-Benutzerhandbuch.

Einschränken von Netzwerkzugriff

Ein GuardDuty Ergebnis kann darauf hindeuten, dass auf eine Datenbank auch außerhalb Ihrer Anwendungen oder Virtual Private Cloud (VPC) zugegriffen werden kann. Wenn es sich bei der Remote-IP-Adresse in der Erkenntnis um eine unerwartete Verbindungsquelle handelt, überprüfen Sie die Sicherheitsgruppen. Eine Liste der an die Datenbank angehängten Sicherheitsgruppen ist in der https://console.aws.amazon.com/rds/Konsole unter Sicherheitsgruppen oder in der JSON-Datei `resource.rdsDbInstanceDetails.dbSecurityGroups` der Ergebnisse verfügbar. Weitere Informationen zur Konfiguration von Sicherheitsgruppen finden Sie unter Zugriffskontrolle mit Sicherheitsgruppen im Amazon-RDS-Benutzerhandbuch.

Wenn Sie eine Firewall verwenden, schränken Sie den Netzwerkzugriff auf die Datenbank ein, indem Sie die Network Access Control Lists (NACLs) neu konfigurieren. Weitere Informationen finden Sie unter Firewall-Richtlinien in AWS Network Firewall im Entwicklerhandbuch für AWS Network Firewall .

Behebung einer potenziell gefährdeten Lambda-Funktion

Bei der GuardDuty Lambda-Protection-Erkenntnistypen Generierung ist Ihre Lambda-Funktion möglicherweise beeinträchtigt. Wenn die Aktivität, die GuardDuty zu diesem Ergebnis geführt hat, erwartet wurde, können Sie die Verwendung von. Unterdrückungsregeln Wir empfehlen, die folgenden Schritte durchzuführen, um eine beeinträchtigte Lambda-Funktion zu beheben:

So beheben Sie Erkenntnisse von Lambda Protection

1. Identifizieren Sie die potenziell gefährdete Lambda-Funktionsversion.

   Ein GuardDuty Ergebnis für Lambda Protection enthält den Namen, den Amazon-Ressourcennamen (ARN), die Funktionsversion und die Revisions-ID, die mit der Lambda-Funktion verknüpft sind, die in den Ergebnisdetails aufgeführt sind.
2. Identifizieren Sie die Quelle der potenziell verdächtigen Aktivität.

   a. Überprüfen Sie den Code, der der Lambda-Funktionsversion zugeordnet ist, die an der Erkenntnis beteiligt war.
   b. Überprüfen Sie die importierten Bibliotheken und Ebenen der Lambda-Funktionsversion, die an der Erkenntnis beteiligt waren.
   c. Wenn Sie AWS Lambda Scanfunktionen mit Amazon Inspector aktiviert haben, überprüfen Sie die Ergebnisse von Amazon Inspector im Zusammenhang mit der Lambda-Funktion, die an dem Ergebnis beteiligt war.
   d. Überprüfen Sie die AWS CloudTrail Protokolle, um den Principal zu identifizieren, der das Funktionsupdate verursacht hat, und stellen Sie sicher, dass die Aktivität autorisiert oder erwartet wurde.
3. Korrigieren Sie die potenziell gefährdete Lambda-Funktion.

   a. Deaktivieren Sie die Ausführungsauslöser der Lambda-Funktion, die an der Erkenntnis beteiligt sind. Weitere Informationen finden Sie unter DeleteFunctionEventInvokeConfig.
   b. Überprüfen Sie den Lambda-Code und aktualisieren Sie die Bibliotheksimporte und Lambda-Funktionsschichten, um die potenziell verdächtigen Bibliotheken und Schichten zu entfernen.
   c. Mindern Sie die Ergebnisse von Amazon Inspector im Zusammenhang mit der Lambda-Funktion, die an der Erkenntnis beteiligt war.

Überwachung der GuardDuty Nutzung und Schätzung der Kosten

GuardDuty bietet Nutzungsmetriken, mit denen die Verarbeitung von Schutzplänen, Datenquellen logs/events und vCPUs, die über die GuardDuty Laufzeit überwacht werden, im Laufe der Zeit nachverfolgt wird.

Auf dieser Seite:

- CloudWatch Amazon-Nutzungsmetriken
- Grundlegendes GuardDuty zur Nutzung
- Schätzung der Kosten GuardDuty

CloudWatch Amazon-Nutzungsmetriken

GuardDuty veröffentlicht Nutzungsmetriken bei Amazon CloudWatch, sodass Sie:

- Verfolgen Sie die tatsächliche Nutzung im Laufe der Zeit
- Erstellen Sie benutzerdefinierte Dashboards und Alarme
- Exportieren Sie Nutzungsdaten zur Kostenschätzung im Preisrechner AWS

GuardDuty Nutzungsmetriken werden auf der Grundlage Ihrer Kontokonfiguration veröffentlicht:

- Alle Konten (eigenständige Konten, Konten für delegierte Administratoren und Mitgliedskonten) erhalten individuelle Kennzahlen zur Kontonutzung in Amazon CloudWatch
- Delegierte Administratorkonten erhalten zusätzlich aggregierte Nutzungskennzahlen für das gesamte Unternehmen

GuardDuty Nutzungsmetriken werden CloudWatch innerhalb von 24 Stunden in Amazon veröffentlicht.

Angaben zur Metrik

GuardDuty veröffentlicht die folgenden Nutzungsmetriken `Hourly` für Amazon CloudWatch unter dem `AWS/GuardDuty` Namespace:

Schutzplan	Datenquelle	Metrikname	Einheit	Beschreibung
Grundlegende Bedrohung serkennung	CloudTrailEvents	AnalyzedCount	Anzahl	Anzahl der analysierten CloudTrail Managemen tereignisse
Grundlegende Bedrohung serkennung	VPCFlowLo gDNSLogEvents	AnalyzedBytes	Bytes	Umfang der analysierten VPC-Flow- und DNS-Logs
EKS Protection	Kubernete sAuditLogs	AnalyzedCount	Anzahl	Anzahl der analysierten Amazon EKS-Auditprotokoll ereignisse
S3 Protection	S3DataEvents	AnalyzedCount	Anzahl	Anzahl der analysierten S3-Datenereignisse
Laufzeitü berwachung	RuntimeMo nitoringEC2	Monitored VcpuHours	Anzahl (vCPU-Hours)	EC2-vCPU-Stunden, die von Runtime Monitoring überwacht werden
Laufzeitü berwachung	RuntimeMo nitoringEKS	Monitored VcpuHours	Zählen (vCPU-Hours)	Amazon EKS vCPU-Stun den, die durch Runtime Monitoring überwacht werden

Laufzeitüberwachung	RuntimeMonitoringFargate	MonitoredVcpuHours	Anzahl (vCPU-Hours)	Fargate vCPU-Stunden, die durch Runtime Monitoring überwacht werden
Malware-Schutz für EC2	OnDemandEBSSnapshot	ScannedBytes	Bytes	Menge der gescannten EBS-Snapshot-Daten auf Abruf
Malware-Schutz für EC2	OnDemandEBSVolume	ScannedBytes	Bytes	Menge der gescannten EBS-Volumendaten auf Abruf
Malware-Schutz für EC2	MalwareProtectionEBS	ScannedBytes	Bytes	Menge der von Malware Protection gescannten EBS-Daten
RDS Protection	RDS	MonitoredAcuHours	Anzahl () ACU-Hours	Überwachte Amazon RDS Aurora-Kapazitätseinheiten
RDS Protection	RDS grenzenlos	MonitoredAcuHours	Anzahl () ACU-Hours	Amazon RDS Aurora Überwachte ACU-Stunden ohne Limit

RDS Protection	AuroraScaleout	Monitored AcuHours	Anzahl () ACU-Hours	Überwachte ACU-Stunden von Aurora Scaleout
RDS Protection	RDS	Monitored VcpuHours	Anzahl (v) CPU-Hours	Überwachte Amazon RDS vCPU-Stunden
Lambda Protection	LambdaNetworkLogs	AnalyzedBytes	Bytes	Umfang der analysierten Lambda-Netzwerkprotokolle
KI-Schutz	AIDataEvents	AnalyzedBytes	Bytes	Umfang der analysierten KI-Datenereignisse

Metriken und Dimensionen

- Alle Konten (eigenständige Konten, Konten für delegierte Administratoren und Mitgliedskonten): Zu den Metriken gehören die `DataSource` Dimensionen `AccountId` und.
- Delegierte Administratorkonten: Zu den Metriken gehören auch aggregierte `DataSource` Dimensionen für alle Mitgliedskonten in der Organisation.

Malware-Schutz für S3

GuardDuty `Malware Protection for S3`Der Schutzplan veröffentlicht die folgenden Nutzungskennzahlen für Amazon CloudWatch unter dem `AWS/GuardDuty/MalwareProtection` Namespace:

Metrikname	Einheit	Beschreibung
CompletedScanCount	Anzahl	Die Anzahl der S3-Objekt-Malware-Scans, die in

		einem bestimmten Zeitraum abgeschlossen wurden.
FailedScanCount	Anzahl	Die Anzahl der S3-Objekt -Malware-Scans, die in einem bestimmten Zeitraum fehlgeschlagen sind.
SkippedScanCount	Anzahl	Die Anzahl der S3-Objekt -Malware-Scans, die in einem bestimmten Zeitraum übersprungen wurden.
InfectedScanCount	Anzahl	Die Anzahl der S3-Objekt-Malware-Scans, bei denen in einem bestimmten Zeitraum potenziell schädliche Objekte entdeckt wurden.
CompletedScanBytes	Anzahl	Die Anzahl der in einem bestimmten Zeitraum gescannten S3-Objektbytes.

Metriken: Dimensionen

- Alle Metriken beinhalten `Malware Protection Plan Id, Resource Name` Dimensionen
- SkippedScanCount Die Metrik `Skipped Reason` wird als zusätzliche Dimension hinzugefügt

Grundlegendes GuardDuty zur Nutzung

GuardDuty Verarbeitung von Ereignissen

Wenn diese Option aktiviert ist, GuardDuty werden Ereignisse und Protokolle automatisch direkt aus den von Ihnen ausgewählten AWS-Region Protokollquellen abgerufen. GuardDuty Nimmt Ereignisse aus separaten, unabhängigen Datenquellen auf und bietet so einen umfassenden Sicherheitswert.

> **Important**
>
> Ihre individuellen Service-Log-Konfigurationen oder Filterregeln (für VPC-Flow-Logs, DNS-Logs, CloudTrail Events, S3-Datenereignisse, Kubernetes-Auditprotokolle und Lambda-Netzwerkprotokolle) haben keinen Einfluss auf die verarbeiteten Daten. logs/events GuardDuty

GuardDuty Gebühren für die Verarbeitung von VPC Flow Logs für Instanzen, die von Runtime Monitoring überwacht werden GuardDuty

Für Instances, die von GuardDuty Runtime Monitoring überwacht werden (entweder über den EC2 Runtime Agent oder den Amazon EKS Runtime Agent), GuardDuty fallen keine Gebühren für die Verarbeitung von VPC Flow Logs an, solange der Agent aktiv Laufzeitereignisdaten sendet. Wenn der Agent die Übertragung von Ereignisdaten beendet, GuardDuty kehrt er zur Abrechnung über VPC Flow Logs zurück.

Die Aktivierung von Runtime Monitoring verringert die Nutzung von VPC Flow Logs in GuardDuty Amazon-Nutzungsmetriken CloudWatch . Durch die Deaktivierung von Runtime Monitoring wird die Nutzung von VPC Flow Logs wiederhergestellt.

Schätzung der Kosten GuardDuty

GuardDuty bietet für die meisten Schutzpläne eine kostenlose 30-Tage-Testversion pro AWS Konto an. Während dieser Testphase können Sie:

- Überwachen Sie Ihre tatsächliche Nutzung anhand von GuardDuty Nutzungsmetriken
- Schätzen Sie Ihre monatlichen Kosten mithilfe des AWS Preisrechners auf der Grundlage Ihrer beobachteten Nutzungsmuster

Die folgenden Schutzpläne beinhalten eine kostenlose 30-Tage-Testversion:

- Grundlegende Bedrohungserkennung
- S3 Protection
- EKS Protection
- Laufzeitüberwachung

- RDS Protection
- Lambda Protection
- KI-Schutz
- Malware-Schutz für EC2 (nur für GuardDuty-initiated Scans, wenn Foundational Threat Detection aktiviert ist)

Verwenden AWS Preiskalkulator

Mit dem AWS Preisrechner können Sie Ihre monatlichen GuardDuty Kosten auf der Grundlage Ihrer beobachteten Nutzungsmuster schätzen. Um eine Schätzung zu erstellen für GuardDuty:

1. Öffnen Sie den AWS Preisrechner.
2. Wählen Sie Create estimate (Schätzung erstellen) aus.
3. Suchen Sie auf der Seite Service hinzufügen nach Amazon GuardDuty und wählen Sie Konfigurieren aus.
4. Wählen Sie aus AWS-Region , wo aktiviert GuardDuty ist.
5. Geben Sie im Abschnitt Serviceeinstellungen Ihre geschätzte Nutzung für jeden Schutzplan ein, basierend auf den in Amazon CloudWatch oder der GuardDuty Konsole beobachteten Nutzungsmetriken.
6. Wählen Sie Zu meiner Schätzung hinzufügen aus, um die voraussichtlichen monatlichen Kosten anzuzeigen.

> **Note**
>
> Einige GuardDuty Nutzungsmetriken werden in Byte angegeben. Wenn Sie Werte in den AWS Preisrechner eingeben, müssen Sie möglicherweise Byte in die entsprechende Einheit (MB, GB oder TB) umrechnen. Verwenden Sie die folgenden Umrechnungen:
>
> - 1 MB = 1.048.576 Byte
> - 1 GB = 1.073.741.824 Byte
> - 1 TB = 1.099.511.627.776 Byte

Security Hub-Kunden

Security Hub bietet mit seinem zusätzlichen GuardDuty Threat Analytics-Paket ein vereinfachtes Preismodell für Threat Detection, das die Erfassung mehrerer GuardDuty DataSources Bedrohungen konsolidiert. Bei Verwendung des Security Hub Threat Analytics-Plans (Security Hub mit GuardDuty):

- Mehrere GuardDuty DataSources werden konsolidiert
- Der Einfachheit halber werden Amazon EKS Audit Logs-Ereignisse und S3 Data-Ereignisse mit einer festen Konvertierungsrate in GB umgerechnet.

Informationen zur Erstellung eines Security Hub-Kostenvoranschlags finden Sie in der AWS Security Hub-Dokumentation.

Hinweis: GuardDuty Der kostenlose 30-Tage-Teststatus ist unabhängig von der Security Hub-Integration. Security Hub aktivieren oder deaktivieren:

- Gewährt keine neue kostenlose Testversion, wenn Sie die Testphase bereits genutzt GuardDuty haben
- Unterbricht oder startet eine laufende kostenlose Testversion nicht neu
- Verlängert nicht bestehende Testzeiträume

Funktionsnamen für Schutzpläne in der GuardDuty API

Wenn Sie Amazon GuardDuty zum ersten Mal aktivieren, wird die Verarbeitung Grundlegende Datenquellen in Ihrer AWS Umgebung gestartet. GuardDuty verwendet diese Datenquellen, um einen unabhängigen Ereignisstrom wie VPC-Flussprotokolle, DNS-Protokolle und AWS CloudTrail Verwaltungsereignisse zu verarbeiten. Anschließend analysiert es diese Ereignisse, um potenzielle Sicherheitsbedrohungen zu identifizieren, und generiert Erkenntnisse in Ihrem Konto.

Wenn ein oder mehrere Schutzpläne aktiviert sind, GuardDuty verwendet es zusätzliche Daten von anderen AWS Diensten in Ihrer AWS Umgebung, um potenzielle Sicherheitsbedrohungen zu überwachen und zu analysieren. Diese zusätzlichen Datenquellen werden als Funktionen bezeichnet.

Wechseln Sie von Datenquellen zu Funktionen

Wenn Sie zusätzliche GuardDuty Schutzmaßnahmen wie S3-Schutz, Runtime Monitoring, Lambda-Schutz und andere hinzufügen, können Sie die GuardDuty Funktion entsprechend dem Schutzplan konfigurieren. In der Vergangenheit wurden GuardDuty Schutzmaßnahmen `dataSources` in den APIs aufgerufen. Nach März 2023 werden neue GuardDuty Schutzpläne nun jedoch als `features` und nicht `dataSources` konfiguriert. GuardDuty unterstützt weiterhin die Konfiguration von Schutzplänen, die vor März 2023 eingeführt wurden, wie `dataSources` über die API, aber neue Schutzpläne sind nur als verfügbar`features`. Informationen darüber, welche Schutzpläne betroffen sind, finden Sie unterGuardDuty API-Änderungen.

Wenn Sie GuardDuty Konfiguration und Schutzpläne über die Konsole verwalten, sind Sie von dieser Änderung nicht direkt betroffen und müssen keine Maßnahmen ergreifen. Diese Änderung wirkt sich auf das Verhalten der APIs aus, die zur Aktivierung aufgerufen werden, GuardDuty oder auf die darin enthaltenen Schutzpläne. GuardDuty Wenn Sie APIs verwenden oder AWS CLI um die Konfiguration eines Schutzplans zu aktivieren oder zu bearbeiten, müssen Sie den zugehörigen Funktionsnamen verwenden. Weitere Informationen finden Sie unter Zuordnung von `dataSources` zu `features`.

GuardDuty API-Änderungen im März 2023

Die GuardDuty APIs konfigurieren Schutzfunktionen, die nicht zur Liste der gehörenGuardDuty grundlegende Datenquellen. Ein Funktionsobjekt enthält Funktionsdetails wie Funktionsname und Status und kann zusätzliche Konfigurationen für einige Schutzpläne enthalten. Diese Migration wirkt sich auf die folgenden APIs in der Amazon GuardDuty API-Referenz aus:

- CreateDetector
- GetDetector
- UpdateDetector
- GetMemberDetectors
- UpdateMemberDetectors
- DescribeOrganizationConfiguration
- UpdateOrganizationConfiguration
- GetRemainingFreeTrialDays
- GetUsageStatistics

Funktionen im Vergleich zu Datenquellen

In der Vergangenheit wurden alle GuardDuty Funktionen über ein `dataSources` Objekt in der API übergeben. Ab März 2023 GuardDuty bevorzugt `features` das Objekt anstelle des `dataSources` Objekts in der API. Alle früheren Datenquellen verfügen über entsprechende Feature, aber neuere Feature verfügen möglicherweise nicht über entsprechende Datenquellen.

Die folgende Liste zeigt den Vergleich zwischen einem `dataSources`-Objekt und einem `features`-Objekt, wenn es über eine API übergeben wird:

- Das `dataSources`-Objekt enthält Objekte für jeden Schutztyp und seinen Status. Das `features` Objekt ist eine Liste verfügbarer Funktionen, die jedem darin enthaltenen Schutztyp entsprechen GuardDuty.

  Ab März 2023 ist die Aktivierung von Funktionen die einzige Möglichkeit, neue GuardDuty Funktionen in Ihrer AWS Umgebung zu konfigurieren.
- Das `dataSources` Schema in der API-Anfrage oder -Antwort GuardDuty ist AWS-Region in allen verfügbaren Bereichen dasselbe. Möglicherweise sind nicht alle Feature von in jeder Region verfügbar. Daher können sich die Namen der verfügbaren Feature je nach Region unterscheiden.

Verstehen, wie APIs mit Funktionen funktionieren

Die GuardDuty APIs geben weiterhin ein `dataSources` Objekt zurück, sofern zutreffend, und sie geben auch ein `features` Objekt zurück, das dieselben Informationen in einem anderen Format enthält. GuardDuty Funktionen, die vor März 2023 eingeführt wurden, werden über `dataSources`

Objekt und `features` Objekt verfügbar sein. GuardDuty Funktionen, die seit März 2023 eingeführt wurden, werden nur über das `features` Objekt verfügbar sein. Sie können in derselben API-Anfrage keinen Detektor erstellen oder aktualisieren oder beschreiben, dass Sie beides `dataSources` und die `features` Objektnotation AWS Organizations verwenden. Um GuardDuty Schutztypen zu aktivieren, müssen Sie Ihre vorhandenen Datenquellen auf das `features` Objekt migrieren, indem Sie dieselben APIs verwenden, die jetzt auch das `features` Objekt enthalten.

> **Note**
>
> GuardDuty fügt nach dieser Änderung keine neue Datenquelle hinzu.

GuardDuty hat die Verwendung von Datenquellen, die mit den Schutzplänen verknüpft sind, als veraltet eingestuft. Es unterstützt jedoch weiterhin die GuardDuty grundlegende Datenquellen. Die GuardDuty bewährten Methoden empfehlen die Verwendung von Funktionen zur Aktivierung oder Bearbeitung der Konfiguration für jeden Schutzplan in Ihrem Konto.

Integration von Funktionsänderungen in APIs

- Wenn Sie GuardDuty Konfigurationen über APIs, SDKs oder CloudFormation Vorlagen verwalten und potenzielle neue GuardDuty Funktionen aktivieren möchten, müssen Sie Ihren Code bzw. Ihre Vorlage ändern. Weitere Informationen finden Sie in der Amazon GuardDuty API-Referenz zu den aktualisierten APIs.
- Für GuardDuty Funktionen, die vor diesem Upgrade konfiguriert wurden, können Sie die APIs, SDKs oder die CloudFormation Vorlage weiterhin verwenden. Wir empfehlen jedoch, zur Verwendung von `feature`-Objekt zu wechseln.

  Alle Datenquellen haben ein äquivalentes Feature-Objekt. Weitere Informationen finden Sie unter Zuordnung von `dataSources` zu `features`.
- Derzeit ist `additionalConfiguration` im `features`-Objekt nur für bestimmte Schutzarten verfügbar.
  - Für solche Schutztypen gilt: Wenn Ihre Funktion auf eingestellt `AdditionalConfiguration` `status` ist, die Konfiguration Ihrer Funktion `ENABLED` jedoch nicht aktiviert `status` ist`ENABLED`, GuardDuty werden in diesem Fall keine Maßnahmen ergriffen.
  - Die folgenden APIs sind davon betroffen:
    - UpdateDetector
    - UpdateMemberDetectors

- UpdateOrganizationConfiguration

Zuordnung von **`dataSources`** zu **`features`**

Die folgende Tabelle zeigt die Zuordnung der Schutztypen, `dataSources` und `features`.

GuardDuty Art des Schutzes	Name der Datenquelle *	Feature name
VPC Flow Logs	`flowLogs` (schreibgeschützt; kann nicht geändert werden)	`FLOW_LOGS` (schreibgeschützt; kann nicht geändert werden)
Route53 Resolver DNS-Abfrageprotokolle	`dnsLogs` (schreibgeschützt; kann nicht geändert werden)	`DNS_LOGS` (schreibg eschützt; kann nicht geändert werden)
CloudTrail Ereignisse	`cloudTrail` (schreibgeschützt; kann nicht geändert werden)	`CLOUD_TRAIL` (schreibgeschützt; kann nicht geändert werden)
S3	`s3Logs`	`S3_DATA_EVENTS`
EKS-Schutz	`kubernetes.auditlogs`	`EKS_AUDIT_LOGS`
Malware-Schutz für EC2	`malwareProtection.scanEc2In stanceWithFindings.ebsVolumes`	`EBS_MALWA RE_PROTECTION`
RDS-Anmeldeereignisse	GuardDuty bietet nur Unterstüt zung für die Aktivierung von Funktionen für diese Schutztypen.	`RDS_LOGIN _EVENTS`
EKS-Laufzeit-Überw achung		`EKS_RUNTI ME_MONITORING`
Laufzeitüberwachung		`RUNTIME_M ONITORING`

GuardDuty Art des Schutzes	Name der Datenquelle *	Feature name
GuardDuty Sicherheitsagent für Amazon EKS-Cluster		EKS_RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT
GuardDuty Sicherheitsagent für ECS-Fargate Amazon-Cluster		RUNTIME_MONITORING.additionalConfiguration.ECS_FARGATE_AGENT_MANAGEMENT
GuardDuty Sicherheitsagent für Amazon EC2 EC2-Instances		RUNTIME_MONITORING.additionalConfiguration.EC2_AGENT_MANAGEMENT

GuardDuty Art des Schutzes	Name der Datenquelle *	Feature name
Lambda Protection		LAMBDA_NETWORK_LOGS

* GetUsageStatistics verwendet seine eigenen `dataSource`-Namen. Für weitere Informationen siehe Überwachung der GuardDuty Nutzung und Schätzung der Kosten oder GetUsageStatistics.

Sicherheit bei Amazon GuardDuty

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der geteilten Verantwortlichkeit beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Third-party Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS und . Weitere Informationen zu den Compliance-Programmen, die für gelten GuardDuty, finden Sie unter AWS Leistungen im Umfang nach Compliance-Programmen AWS .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, einschließlich der Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Nutzung anwenden können GuardDuty. Es zeigt Ihnen, wie Sie die Konfiguration vornehmen GuardDuty , um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Sie bei der Überwachung und Sicherung Ihrer GuardDuty Ressourcen unterstützen.

Inhalt

- Datenschutz bei Amazon GuardDuty
- GuardDuty Amazon-API-Aufrufe protokollieren mit AWS CloudTrail
- Identity and Access Management für Amazon GuardDuty
- Konformitätsüberprüfung für Amazon GuardDuty
- Resilienz bei Amazon GuardDuty
- Infrastruktursicherheit bei Amazon GuardDuty
- Amazon GuardDuty - und Schnittstellen-VPC-Endpunkte ()AWS PrivateLink

Datenschutz bei Amazon GuardDuty

Das Modell der AWS https://aws.amazon.com/compliance/shared-responsibility-model/ gilt für den Datenschutz bei Amazon GuardDuty. Wie in diesem Modell beschrieben, AWS ist es für den Schutz der globalen Infrastruktur verantwortlich, auf der das gesamte System läuft AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz in der Region . Weitere Informationen zum Datenschutz in Europa finden Sie im Zentrum für die Datenschutz-Grundverordnung (DSGVO).

Aus Datenschutzgründen empfehlen wir, Ihre AWS-Konto Anmeldeinformationen zu schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einzurichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten findest du unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit der Konsole, der API GuardDuty oder den SDKs arbeiten oder diese auf andere Weise AWS-Services verwenden. AWS CLI AWS Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet

werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Verschlüsselung im Ruhezustand

Alle GuardDuty Kundendaten werden im Ruhezustand mithilfe von AWS Verschlüsselungslösungen verschlüsselt.

GuardDuty Daten, wie z. B. Befunde, werden im Ruhezustand mithilfe von AWS Key Management Service (AWS KMS) mit AWS eigenen Schlüsseln verschlüsselt.

Verschlüsselung während der Übertragung

GuardDuty analysiert Protokolldaten von anderen Diensten. GuardDuty verschlüsselt alle Daten während der Übertragung von diesen Services mit HTTPS und KMS. Sobald die benötigten Informationen aus den Protokollen GuardDuty extrahiert wurden, werden sie verworfen. Weitere Informationen zur GuardDuty Verwendung von Informationen aus anderen Diensten finden Sie unter GuardDuty Datenquellen.

GuardDuty Daten werden bei der Übertragung zwischen Diensten verschlüsselt.

Abmeldung von der Verwendung Ihrer Daten zur Serviceverbesserung

Sie können die Verwendung Ihrer Daten für die Entwicklung GuardDuty und Verbesserung anderer AWS Sicherheitsdienste ablehnen, indem Sie die AWS Organizations Opt-Out-Richtlinie verwenden. Sie können sich auch dann abmelden, wenn diese Daten derzeit GuardDuty nicht erfasst werden. Weitere Informationen zur Deaktivierung finden Sie in den Opt-Out-Richtlinien für KI-Services im Benutzerhandbuch für AWS Organizations .

> **Note**
>
> Damit Sie die Opt-Out-Richtlinie nutzen können, müssen Ihre AWS Konten zentral von verwaltet werden AWS Organizations. Falls Sie noch keine Organisation für Ihre AWS Konten erstellt haben, finden Sie weitere Informationen unter Organisation erstellen und verwalten im AWS Organizations Benutzerhandbuch.

Opt-Out hat folgende Auswirkungen:

- GuardDuty löscht die Daten, die vor Ihrer Abmeldung zur Serviceverbesserung erfasst und gespeichert wurden (falls vorhanden).
- Nach Ihrer Abmeldung GuardDuty werden diese Daten nicht mehr zu Zwecken der Serviceverbesserung erfasst oder gespeichert.

In den folgenden Themen wird erläutert, wie die einzelnen Funktionen GuardDuty möglicherweise Ihre Daten zur Serviceverbesserung verarbeiten.

Inhalt

- GuardDuty Überwachung der Laufzeit
- GuardDuty Schutz vor Schadsoftware

GuardDuty Überwachung der Laufzeit

GuardDuty Runtime Monitoring ermöglicht die Laufzeiterkennung von Bedrohungen für Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster, nur AWS Fargate Amazon Elastic Container Service (Amazon ECS), und Amazon Elastic Compute Cloud (Amazon EC2) -Instances in Ihrer Umgebung. AWS Nachdem Sie Runtime Monitoring aktiviert und den GuardDuty Security Agent für Ihre Ressource bereitgestellt haben, GuardDuty beginnt die Überwachung und Analyse der mit Ihrer Ressource verbundenen Laufzeitereignisse. Zu diesen Runtime-Ereignistypen gehören Prozessereignisse, Container-Ereignisse, DNS-Ereignisse und mehr. Weitere Informationen finden Sie unter Gesammelte Runtime-Ereignistypen, die GuardDuty verwendet.

GuardDuty sammelt sowohl Befehle (wie `curl`systemctl, und`cron`) als auch die zugehörigen Argumente (wie`start`,`stop`,`disable`) aus Ihren Workloads. GuardDuty Erfasst beispielsweise sowohl den Befehl `systemctl` als auch die zugehörigen Argumente `systemctl stop` *`service-name`*`stop` *`service-name`*, wenn jemand ausgeführt wird. Diese detaillierten Informationen helfen bei GuardDuty der Erkennung komplexer Bedrohungen, indem Befehlsmuster analysiert und mehrere Ereignisse miteinander in Beziehung gesetzt werden. GuardDutyKann beispielsweise erkennen, wenn ein Angreifer versucht, Sicherheitsdienste zu deaktivieren, oder bekannte schädliche Dateien ausführt. Es verwendet diese Daten zwar GuardDuty aktiv zur Erkennung von Bedrohungen, verwendet diese Befehle und Argumente jedoch derzeit nicht zur Serviceverbesserung (dies könnte in Zukunft der Fall sein). Ihr Vertrauen, Ihre Privatsphäre und die Sicherheit Ihrer Inhalte haben für uns höchste Priorität und wir stellen sicher, dass unsere Nutzung unseren Verpflichtungen Ihnen gegenüber entspricht. Weitere Informationen finden Sie unter Häufig gestellte Fragen zum Datenschutz.

GuardDuty Schutz vor Schadsoftware

GuardDuty Der Malware-Schutz scannt und erkennt Malware in EBS-Volumes, die an Ihre potenziell gefährdeten Amazon EC2-Instance- und Container-Workloads angehängt sind, neu hochgeladene Dateien in Ihren ausgewählten Amazon S3-Buckets und Backup-Ressourcen. Sammelt oder verwendet erkannte Malware derzeit GuardDuty nicht zur Serviceverbesserung. Wenn GuardDuty Malware Protection jedoch in Zukunft eine EBS-Volume-Datei, eine Backup-Datei oder eine S3-Datei als bösartig oder schädlich identifiziert, sammelt und speichert GuardDuty Malware Protection diese Datei, um die Malware-Erkennung und den GuardDuty Service weiterzuentwickeln und zu verbessern. Diese gesammelten Daten können auch zur Entwicklung und Verbesserung anderer AWS -Sicherheitsservices verwendet werden. Ihr Vertrauen, Ihre Privatsphäre und die Sicherheit Ihrer Inhalte haben für uns höchste Priorität und wir stellen sicher, dass unsere Nutzung unseren Verpflichtungen Ihnen gegenüber entspricht. Weitere Informationen finden Sie unter Häufig gestellte Fragen zum Datenschutz.

GuardDuty Amazon-API-Aufrufe protokollieren mit AWS CloudTrail

Amazon GuardDuty ist in einen Service integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Service in ausgeführt wurden GuardDuty. CloudTrail erfasst alle API-Aufrufe GuardDuty als Ereignisse, einschließlich Aufrufe von der GuardDuty Konsole und von Codeaufrufen an die GuardDuty APIs. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon Simple Storage Service (Amazon S3) -Bucket aktivieren, einschließlich Ereignissen für GuardDuty. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, an die die Anfrage gestellt wurde GuardDuty, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen dazu CloudTrail, einschließlich der Konfiguration und Aktivierung, finden Sie im AWS CloudTrail Benutzerhandbuch.

GuardDuty Informationen in CloudTrail

CloudTrail ist in Ihrem AWS Konto aktiviert, wenn Sie das Konto erstellen. Wenn unterstützte Ereignisaktivitäten in auftreten GuardDuty, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen im CloudTrail Ereignisverlauf in einem Ereignis aufgezeichnet. Sie können

aktuelle Ereignisse in Ihrem AWS Konto ansehen, suchen und herunterladen. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS Konto, einschließlich der Ereignisse für GuardDuty, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie ein Trail in der Konsole anlegen, gilt dieser für alle Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie unter:

- Übersicht zum Erstellen eines Trails
- In CloudTrail unterstützte Services und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Anmeldeinformationen des Root-Benutzers oder des IAM-Benutzers gestellt wurde
- Ob die Anfrage mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen föderierten Benutzer ausgeführt wurde
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

GuardDuty Ereignisse auf der Kontrollebene in CloudTrail

Standardmäßig CloudTrail protokolliert es alle GuardDuty API-Operationen, die in der Amazon GuardDuty API-Referenz bereitgestellt werden, als Ereignisse in CloudTrail Dateien.

GuardDuty Datenereignisse in CloudTrail

GuardDuty Überwachung der Laufzeitverwendet einen GuardDuty Sicherheitsagenten, der auf Ihren Amazon Elastic Kubernetes Service (Amazon EKS) -Clustern, Amazon Elastic Compute Cloud (Amazon EC2) -Instances und AWS Fargate (nur Amazon Elastic Container Service (Amazon ECS)) Aufgaben installiert ist, um Add-on (`aws-guardduty-agent`) zu sammeln, die Gesammelte Laufzeit-Ereignistypen für Ihre AWS Workloads gesammelt werden, und sendet sie dann zur Bedrohungserkennung und GuardDuty -analyse an.

Protokollierung und Überwachung von Datenereignissen

Sie können die AWS CloudTrail Protokolle optional so konfigurieren, dass die Datenereignisse für Ihren Security Agent angezeigt werden. GuardDuty

Informationen zur Erstellung und Konfiguration CloudTrail finden Sie im AWS CloudTrail Benutzerhandbuch unter Datenereignisse. Folgen Sie den Anweisungen zur Protokollierung von Datenereignissen mit erweiterten Ereignisauswahlmöglichkeiten in der AWS-Managementkonsole. Wenn Sie den Trail protokollieren, stellen Sie sicher, dass Sie die folgenden Änderungen vornehmen:

- Wählen Sie für den Ereignistyp „Daten“ die Option GuardDutyDetektor aus.
- Wählen Sie für die Protokollauswahlvorlage die Option Alle Ereignisse protokollieren aus.
- Erweitern Sie die JSON-Ansicht für die Konfiguration. Die Ausgabe sollte ähnlich dem folgenden JSON aussehen:

```
[
  {
    "name": "",
    "fieldSelectors": [
      {
        "field": "eventCategory",
        "equals": [
          "Data"
        ]
      },
      {
        "field": "resources.type",
        "equals": [
          "AWS::GuardDuty::Detector"
        ]
      }
```

```
    ]
  }
]
```

Nachdem Sie den Selektor für den Trail aktiviert haben, navigieren Sie zur Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/. Sie können die Datenereignisse aus Ihrem S3-Bucket herunterladen, den Sie bei der Konfiguration der CloudTrail Protokolle ausgewählt haben.

Beispiel: Einträge in GuardDuty Protokolldateien

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der das Ereignis auf der Datenebene demonstriert.

```
{
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "111122223333:aws:ec2-instance:i-123412341234example",
            "arn": "arn:aws:sts::111122223333:assumed-role/aws:ec2-
instance/i-123412341234example",
            "accountId": "111122223333",
            "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "111122223333:aws:ec2-instance",
                    "arn": "arn:aws:iam::111122223333:role/aws:ec2-instance",
                    "accountId": "111122223333",
                    "userName": "aws:ec2-instance"
                },
                "attributes": {
                    "creationDate": "2023-03-05T04:00:21Z",
                    "mfaAuthenticated": "false"
                },
```

```
                "ec2RoleDelivery": "2.0"
            }
        },
        "eventTime": "2023-03-05T06:03:49Z",
        "eventSource": "guardduty.amazonaws.com",
        "eventName": "SendSecurityTelemetry",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "54.240.230.177",
        "userAgent": "aws-sdk-rust/0.54.1 os/linux lang/rust/1.66.0",
        "requestParameters": null,
        "responseElements": null,
        "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
        "readOnly": false,
        "resources": [{
            "accountId": "111122223333",
            "type": "AWS::GuardDuty::Detector",
            "ARN": "arn:aws:guardduty:us-
west-2:111122223333:detector/12abc34d567e8fa901bc2d34e56789f0"
        }],
        "eventType": "AwsApiCall",
        "managementEvent": false,
        "recipientAccountId": "111122223333",
        "eventCategory": "Data",
        "tlsDetails": {
            "tlsVersion": "TLSv1.2",
            "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
            "clientProvidedHostHeader": "guardduty-data.us-east-1.amazonaws.com"
        }
    }
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `CreateIPThreatIntelSet` Aktion demonstriert (Ereignis auf der Steuerungsebene).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Alice",
        "accountId": "444455556666",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
```

```
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-06-14T22:54:20Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::444455556666:user/Alice",
                "accountId": "444455556666",
                "userName": "Alice"
            }
        }
    },
    "eventTime": "2018-06-14T22:57:56Z",
    "eventSource": "guardduty.amazonaws.com",
    "eventName": "CreateThreatIntelSet",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "54.240.230.177",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "detectorId": "12abc34d567e8fa901bc2d34e56789f0",
        "name": "Example",
        "format": "TXT",
        "activate": false,
        "location": "https://s3.amazonaws.com/bucket.name/file.txt"
    },
    "responseElements": {
        "threatIntelSetId": "1ab200428351c99d859bf61992460d24"
    },
    "requestID": "5f6bf981-7026-11e8-a9fc-5b37d2684c5c",
    "eventID": "81337b11-e5c8-4f91-b141-deb405625bc9",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "444455556666"
}
```


Aus diesem Ereignis Informationen können Sie ersehen, dass die Anfrage gestellt wurde, um eine Bedrohungsliste `Example` in GuardDuty zu erstellen. Sie können auch sehen, dass die Anfrage von einem Benutzer namens Alice am 14. Juni 2018 gemacht wurde.

Identity and Access Management für Amazon GuardDuty

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Ressourcen zu verwenden. GuardDuty IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

- Zielgruppe
- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien
- So GuardDuty arbeitet Amazon mit IAM
- Identity-based Richtlinienbeispiele für Amazon GuardDuty
- Verwenden von serviceverknüpften Rollen für Amazon GuardDuty
- AWS verwaltete Richtlinien für Amazon GuardDuty
- Fehlerbehebung Amazon GuardDuty Amazon-Identität und Zugriff

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von Ihrer Rolle ab:

- Servicebenutzer – Fordern Sie von Ihrem Administrator Berechtigungen an, wenn Sie nicht auf Features zugreifen können (siehe Fehlerbehebung Amazon GuardDuty Amazon-Identität und Zugriff).
- Serviceadministrator – Bestimmen Sie den Benutzerzugriff und stellen Sie Berechtigungsanfragen (siehe So GuardDuty arbeitet Amazon mit IAM).
- IAM-Administrator – Schreiben Sie Richtlinien zur Zugriffsverwaltung (siehe Identity-based Richtlinienbeispiele für Amazon GuardDuty).

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen sich als IAM-Benutzer authentifizieren oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich als föderierte Identität anmelden, indem Sie Anmeldeinformationen aus einer Identitätsquelle wie AWS IAM Identity Center (IAM Identity Center), Single Sign-On-Authentifizierung oder Anmeldeinformationen verwenden. Google/Facebook Weitere Informationen zum Anmelden finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch für AWS-Anmeldung .

AWS Bietet für den programmatischen Zugriff ein SDK und eine CLI zum kryptografischen Signieren von Anfragen. Weitere Informationen finden Sie unter AWS Signature Version 4 for API requests im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, dem sogenannten AWS-Konto Root-Benutzer, der vollständigen Zugriff auf alle AWS-Services Ressourcen hat. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Eine Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Tasks that require root user credentials im IAM-Benutzerhandbuch.

Verbundidentität

Es hat sich bewährt, dass menschliche Benutzer für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen einen Verbund mit einem Identitätsanbieter verwenden müssen.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensverzeichnis, Ihrem Directory Service Web-Identitätsanbieter oder der AWS-Services mithilfe von Anmeldeinformationen aus einer Identitätsquelle zugreift. Verbundene Identitäten übernehmen Rollen, die temporäre Anmeldeinformationen bereitstellen.

Für die zentrale Zugriffsverwaltung empfehlen wir AWS IAM Identity Center. Weitere Informationen finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center -Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. Wir empfehlen die Verwendung temporärer Anmeldeinformationen anstelle von IAM-Benutzern mit langfristigen Anmeldeinformationen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Erfordern, dass menschliche Benutzer den Verbund mit einem Identitätsanbieter verwenden müssen, um AWS mithilfe temporärer Anmeldeinformationen darauf zugreifen zu können.

Eine IAM-Gruppe spezifiziert eine Sammlung von IAM-Benutzern und erleichtert die Verwaltung von Berechtigungen für große Gruppen von Benutzern. Weitere Informationen finden Sie unter Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität mit spezifischen Berechtigungen, die temporäre Anmeldeinformationen bereitstellt. Sie können eine Rolle übernehmen, indem Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln AWS CLI oder einen AWS API-Vorgang aufrufen. Weitere Informationen finden Sie unter Methoden, um eine Rolle zu übernehmen im IAM-Benutzerhandbuch.

IAM-Rollen sind nützlich für den Verbundbenutzer-Zugriff, temporäre IAM-Benutzerberechtigungen, kontoübergreifenden Zugriff, serviceübergreifenden Zugriff und Anwendungen, die auf Amazon EC2 laufen. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie definiert Berechtigungen, wenn sie mit einer Identität oder Ressource verknüpft sind. AWS bewertet diese Richtlinien, wenn ein Principal eine Anfrage stellt. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Mit Hilfe von Richtlinien legen Administratoren fest, wer Zugriff auf was hat, indem sie definieren, welches Prinzipal welche Aktionen auf welchen Ressourcenund unter welchen Bedingungendurchführen darf.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator erstellt IAM-Richtlinien und fügt sie zu Rollen hinzu, die die Benutzer dann übernehmen können. IAM-Richtlinien definieren Berechtigungen unabhängig von der Methode, die zur Ausführung der Operation verwendet wird.

Identity-based Richtlinien

Identity-based Richtlinien sind Richtliniendokumente für JSON-Berechtigungen, die Sie an eine Identität (Benutzer, Gruppe oder Rolle) anhängen. Diese Richtlinien steuern, welche Aktionen Identitäten für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Identity-based Richtlinien können Inline-Richtlinien (direkt in eine einzelne Identität eingebettet) oder verwaltete Richtlinien (eigenständige Richtlinien, die mehreren Identitäten zugeordnet sind) sein. Informationen dazu, wie Sie zwischen verwalteten und Inline-Richtlinien wählen, finden Sie unter Choose between managed policies and inline policies im IAM-Benutzerhandbuch.

Resource-based Richtlinien

Resource-based Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele hierfür sind Vertrauensrichtlinien für IAM-Rollen und Amazon S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben.

Resource-based Richtlinien sind Inline-Richtlinien, die sich in diesem Dienst befinden. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Weitere Richtlinientypen

AWS unterstützt zusätzliche Richtlinientypen, mit denen die maximalen Berechtigungen festgelegt werden können, die durch gängigere Richtlinientypen gewährt werden:

- Berechtigungsgrenzen – Eine Berechtigungsgrenze legt die maximalen Berechtigungen fest, die eine identitätsbasierte Richtlinie einer IAM-Entität erteilen kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im -IAM-Benutzerhandbuch.
- Service-Kontrollrichtlinien (SCPs) – SCPs legen die maximalen Berechtigungen für eine Organisation oder Organisationseinheit in AWS Organizations fest. Weitere Informationen finden Sie unter Service-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.
- Ressourcen-Kontrollrichtlinien (RCPs) – RCPs definieren die maximale Anzahl an Berechtigungen, die Ressourcen in Ihren Konten zur Verfügung stehen. Weitere Informationen finden Sie unter Ressourcen-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die als Parameter übergeben werden, wenn Sie eine temporäre Sitzung für eine Rolle oder einen Verbundbenutzer erstellen. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere Arten von Richtlinien für eine Anfrage gelten, sind die daraus resultierenden Berechtigungen schwieriger zu verstehen. Informationen darüber, wie AWS bestimmt wird, ob eine

Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie unter Bewertungslogik für Richtlinien im IAM-Benutzerhandbuch.

So GuardDuty arbeitet Amazon mit IAM

Bevor Sie IAM zur Verwaltung des Zugriffs auf verwenden, sollten Sie sich darüber informieren GuardDuty, mit welchen IAM-Funktionen Sie arbeiten können. GuardDuty

IAM-Funktionen, die Sie mit Amazon verwenden können GuardDuty

IAM-Feature	GuardDuty Unterstützung
Identity-based Richtlinien	Ja
Resource-based Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Prinzipalberechtigungen	Ja
Servicerollen	Ja
Service-linked Rollen	Ja

Einen allgemeinen Überblick darüber, wie GuardDuty und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren.

Identity-based Richtlinien für GuardDuty

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identity-based Richtlinien sind Richtliniendokumente für JSON-Berechtigungen, die Sie an eine Identität anhängen können, z. B. an einen IAM-Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Identity-based Richtlinienbeispiele für GuardDuty

Beispiele für GuardDuty identitätsbasierte Richtlinien finden Sie unter. Identity-based Richtlinienbeispiele für Amazon GuardDuty

Resource-based Richtlinien innerhalb GuardDuty

Unterstützt ressourcenbasierte Richtlinien: Nein

Resource-based Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Richtlinienaktionen für GuardDuty

Unterstützt Richtlinienaktionen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Nehmen Sie Aktionen in eine Richtlinie auf, um Berechtigungen zur Ausführung des zugehörigen Vorgangs zu erteilen.

Eine Liste der GuardDuty Aktionen finden Sie unter Von Amazon definierte Aktionen GuardDuty in der Service Authorization Reference.

Bei Richtlinienaktionen wird vor der Aktion das folgende Präfix GuardDuty verwendet:

```
guardduty
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
      "guardduty:action1",
      "guardduty:action2"
         ]
```

Beispiele für GuardDuty identitätsbasierte Richtlinien finden Sie unter. Identity-based Richtlinienbeispiele für Amazon GuardDuty

Politische Ressourcen für GuardDuty

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Als Best Practice geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen

(ARN) an. Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Eine Liste der GuardDuty Ressourcentypen und ihrer ARNs finden Sie unter Von Amazon definierte Ressourcen GuardDuty in der Service Authorization Reference. Informationen darüber, mit welchen Aktionen Sie den ARN jeder Ressource angeben können, finden Sie unter Von Amazon definierte Aktionen GuardDuty.

Beispiele für GuardDuty identitätsbasierte Richtlinien finden Sie unter. Identity-based Richtlinienbeispiele für Amazon GuardDuty

Bedingungsschlüssel für Richtlinien für GuardDuty

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Condition` gibt an, wann Anweisungen auf der Grundlage definierter Kriterien ausgeführt werden. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der GuardDuty Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für Amazon GuardDuty in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Amazon definierte Aktionen GuardDuty.

Beispiele für GuardDuty identitätsbasierte Richtlinien finden Sie unter. Identity-based Richtlinienbeispiele für Amazon GuardDuty

Zugriffskontrolllisten (ACLs) in GuardDuty

Unterstützt ACLs: Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Attribute-based Zugriffskontrolle (ABAC) mit GuardDuty

Unterstützt ABAC (Tags in Richtlinien): Teilweise

Attribute-based Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, die Berechtigungen auf der Grundlage von Attributen definiert, die als Tags bezeichnet werden. Sie können Tags an IAM-Entitäten und AWS -Ressourcen anhängen und dann ABAC-Richtlinien entwerfen, die Operationen zulassen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Temporäre Anmeldeinformationen verwenden mit GuardDuty

Unterstützt temporäre Anmeldeinformationen: Ja

Temporäre Anmeldeinformationen ermöglichen kurzfristigen Zugriff auf AWS Ressourcen und werden automatisch erstellt, wenn Sie einen Verbund verwenden oder die Rollen wechseln. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Anmeldeinformationen in IAM und AWS-Services , die mit IAM funktionieren im IAM-Benutzerhandbuch.

Cross-service Hauptberechtigungen für GuardDuty

Unterstützt Forward Access Sessions (FAS): Ja

Forward Access Sessions (FAS) verwenden die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen AWS-Service an nachgelagerte Dienste zu

stellen. Einzelheiten zu den Richtlinien für FAS-Anforderungen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für GuardDuty

Unterstützt Servicerollen: Ja

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Durch das Ändern der Berechtigungen für eine Servicerolle kann die GuardDuty Funktionalität beeinträchtigt werden. Bearbeiten Sie Servicerollen nur, GuardDuty wenn Sie dazu eine Anleitung erhalten.

Service-linked Rollen für GuardDuty

Unterstützt serviceverknüpfte Rollen: Ja

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer AWS-Service verknüpft ist. Der Dienst kann die Rolle übernehmen, eine Aktion in Ihrem Namen auszuführen. Service-linked Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Einzelheiten zum Erstellen oder Verwalten von GuardDuty dienstbezogenen Rollen finden Sie unterVerwenden von serviceverknüpften Rollen für Amazon GuardDuty.

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie in der Tabelle nach einem Dienst, der einen `Yes` in der Service-linked Rollenspalte enthält. Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Identity-based Richtlinienbeispiele für Amazon GuardDuty

Benutzer und Rollen haben standardmäßig nicht die Berechtigung, GuardDuty-Ressourcen zu erstellen oder zu ändern. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien (Konsole) im IAM-Benutzerhandbuch.

Einzelheiten zu Aktionen und Ressourcentypen, die von definiert wurden GuardDuty, einschließlich des Formats der ARNs für jeden der Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon GuardDuty in der Service Authorization Reference.

Themen

- Best Practices für Richtlinien
- Verwenden der Konsole GuardDuty
- Für die Aktivierung sind Berechtigungen erforderlich GuardDuty
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer
- Benutzerdefinierte IAM-Richtlinie zur Gewährung von schreibgeschütztem Zugriff auf GuardDuty
- Zugriff auf Ergebnisse verweigern GuardDuty
- Verwendung einer benutzerdefinierten IAM-Richtlinie zur Beschränkung des Zugriffs auf Ressourcen GuardDuty

Best Practices für Richtlinien

Identity-based Richtlinien legen fest, ob jemand GuardDuty Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Beachten Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Richtlinien und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien oder Von AWS verwaltete Richtlinien für Auftragsfunktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer

Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.

- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Best Practices für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der Konsole GuardDuty

Um auf die GuardDuty Amazon-Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Informationen zu den GuardDuty Ressourcen in Ihrem Verzeichnis aufzulisten und einzusehen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die GuardDuty Konsole weiterhin verwenden können, fügen Sie den Entitäten auch die GuardDuty `ConsoleAccess` oder die `ReadOnly` AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Für die Aktivierung sind Berechtigungen erforderlich GuardDuty

Um Berechtigungen zu gewähren, über die verschiedene IAM-Identitäten (Benutzer, Gruppen und Rollen) verfügen müssen, fügen Sie die erforderliche AWS verwaltete Richtlinie: AmazonGuardDutyFullAccess_v2 (empfohlen) Richtlinie zur Aktivierung hinzu. GuardDuty

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der API oder. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
```

```
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Benutzerdefinierte IAM-Richtlinie zur Gewährung von schreibgeschütztem Zugriff auf GuardDuty

Um nur Lesezugriff zu gewähren, können GuardDuty Sie die verwaltete Richtlinie verwenden. `AmazonGuardDutyReadOnlyAccess`

Um eine benutzerdefinierte Richtlinie zu erstellen, die einer IAM-Rolle, einem Benutzer oder einer Gruppe schreibgeschützten Zugriff gewährt GuardDuty, können Sie die folgende Anweisung verwenden:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:ListMembers",
                "guardduty:GetMembers",
                "guardduty:ListInvitations",
                "guardduty:ListDetectors",
                "guardduty:GetDetector",
                "guardduty:ListFindings",
                "guardduty:GetFindings",
                "guardduty:ListIPSets",
                "guardduty:GetIPSet",
                "guardduty:ListThreatIntelSets",
                "guardduty:GetThreatIntelSet",
```

```
                "guardduty:GetMasterAccount",
                "guardduty:GetInvitationsCount",
                "guardduty:GetFindingsStatistics",
                "guardduty:DescribeMalwareScans",
                "guardduty:UpdateMalwareScanSettings",
                "guardduty:GetMalwareScanSettings"
            ],
            "Resource": "*"
        }
    ]
}
```

Zugriff auf Ergebnisse verweigern GuardDuty

Sie können die folgende Richtlinie verwenden, um einer IAM-Rolle, einem Benutzer oder einer Gruppe den Zugriff auf GuardDuty Ergebnisse zu verweigern. Benutzer können keine Ergebnisse oder Details zu Ergebnissen anzeigen, aber sie können auf alle anderen GuardDuty Operationen zugreifen:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:CreateDetector",
                "guardduty:DeleteDetector",
                "guardduty:UpdateDetector",
                "guardduty:GetDetector",
                "guardduty:ListDetectors",
                "guardduty:CreateIPSet",
                "guardduty:DeleteIPSet",
                "guardduty:UpdateIPSet",
                "guardduty:GetIPSet",
                "guardduty:ListIPSets",
                "guardduty:CreateThreatIntelSet",
                "guardduty:DeleteThreatIntelSet",
                "guardduty:UpdateThreatIntelSet",
                "guardduty:GetThreatIntelSet",
```

```
                "guardduty:ListThreatIntelSets",
                "guardduty:ArchiveFindings",
                "guardduty:UnarchiveFindings",
                "guardduty:CreateSampleFindings",
                "guardduty:CreateMembers",
                "guardduty:InviteMembers",
                "guardduty:GetMembers",
                "guardduty:DeleteMembers",
                "guardduty:DisassociateMembers",
                "guardduty:StartMonitoringMembers",
                "guardduty:StopMonitoringMembers",
                "guardduty:ListMembers",
                "guardduty:GetMasterAccount",
                "guardduty:DisassociateFromMasterAccount",
                "guardduty:AcceptAdministratorInvitation",
                "guardduty:ListInvitations",
                "guardduty:GetInvitationsCount",
                "guardduty:DeclineInvitations",
                "guardduty:DeleteInvitations"
            ],
            "Resource": "*"
        },
         {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "guardduty.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
        }
```

```
    ]
}
```

Verwendung einer benutzerdefinierten IAM-Richtlinie zur Beschränkung des Zugriffs auf Ressourcen GuardDuty

Um den Zugriff eines Benutzers auf der GuardDuty Grundlage der Detektor-ID zu definieren, können Sie alle GuardDutyAPI-Aktionen in Ihren benutzerdefinierten IAM-Richtlinien verwenden, mit Ausnahme der folgenden Operationen:

- `guardduty:CreateDetector`
- `guardduty:DeclineInvitations`
- `guardduty:DeleteInvitations`
- `guardduty:GetInvitationsCount`
- `guardduty:ListDetectors`
- `guardduty:ListInvitations`

Verwenden Sie die folgenden Operationen in einer IAM-Richtlinie, um den Zugriff eines Benutzers auf der GuardDuty Grundlage der IPSet-ID und -ID zu definieren: ThreatIntelSet

- `guardduty:DeleteIPSet`
- `guardduty:DeleteThreatIntelSet`
- `guardduty:GetIPSet`
- `guardduty:GetThreatIntelSet`
- `guardduty:UpdateIPSet`
- `guardduty:UpdateThreatIntelSet`

Die folgenden Beispiele zeigen, wie Richtlinien mithilfe einiger der vorhergehenden Vorgänge erstellt werden:

- Diese Richtlinie erlaubt einem Benutzer die Ausführung des `guardduty:UpdateDetector`-Vorgangs mithilfe der Detektor-ID 1234567 in der Region „us-east-1“:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:UpdateDetector"
            ],
            "Resource": "arn:aws:guardduty:us-
east-1:123456789012:detector/1234567"
        }
    ]
}
```

- Diese Richtlinie erlaubt einem Benutzer die Ausführung des `guardduty:UpdateIPSet`-Vorgangs mithilfe der Detektor-ID 1234567 und der IPSet-ID 000000 in der Region „us-east-1“:

> **Note**
>
> Stellen Sie sicher, dass der Benutzer über die erforderlichen Berechtigungen für den Zugriff auf vertrauenswürdige IP-Adressen und Bedrohungslisten in verfügt. GuardDuty Weitere Informationen finden Sie unter Voraussetzungen für Entitätslisten und IP-Adresslisten einrichten.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:UpdateIPSet"
            ],
            "Resource": "arn:aws:guardduty:us-
east-1:123456789012:detector/1234567/ipset/000000"
        }
    ]
```

```
}
```

- Diese Richtlinie erlaubt einem Benutzer die Ausführung des `guardduty:UpdateIPSet`-Vorgangs mithilfe einer beliebigen Detektor-ID und der IPSet-ID 000000 in der Region „us-east-1“:

> **Note**
>
> Stellen Sie sicher, dass der Benutzer über die erforderlichen Berechtigungen für den Zugriff auf vertrauenswürdige IP-Adressen und Bedrohungslisten in verfügt GuardDuty. Weitere Informationen finden Sie unter Voraussetzungen für Entitätslisten und IP-Adresslisten einrichten.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:UpdateIPSet"
            ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/*/
ipset/000000"
        }
    ]
}
```

- Diese Richtlinie erlaubt einem Benutzer die Ausführung des `guardduty:UpdateIPSet`-Vorgangs mithilfe der Detektor-ID und einer beliebigen IPSet-ID in der Region „us-east-1“:

> **Note**
>
> Stellen Sie sicher, dass der Benutzer über die erforderlichen Berechtigungen für den Zugriff auf vertrauenswürdige IP-Adressen und Bedrohungslisten in verfügt GuardDuty. Weitere Informationen finden Sie unter Voraussetzungen für Entitätslisten und IP-Adresslisten einrichten.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:UpdateIPSet"
            ],
            "Resource": "arn:aws:guardduty:us-
east-1:123456789012:detector/1234567/ipset/*"
        }
    ]
}
```

Der IAM-Ressourcen-ARN für eine GuardDuty Aktion entspricht dem API-Ressourcenpfad dieser Aktion. Die meisten Aktionen sind dem Detektor oder einer Unterressource zugeordnet. Zum Beispiel `guardduty:GetDetector` Verwendungen und `detector/detectorId` `guardduty:GetFilter` Verwendung`detector/detectorId/filter/filterName`.

Bei den meisten Ergebnissen und Mitgliedsaktionen wird der Operationsname als Suffix an den Ressourcenpfad angehängt. Die Listenoperationen sind die Ausnahme: `guardduty:ListMembers` Sie verwenden die Basis `guardduty:ListFindings` `findings` und `member` Pfade ohne Suffix. Geben Sie den vollständigen Pfad an, wenn Sie eine Richtlinie auf folgende Aktionen beschränken:

- `guardduty:GetFindings`verwendet `detector/detectorId/findings/get`
- `guardduty:GetFindingsStatistics`verwendet `detector/detectorId/findings/statistics`
- `guardduty:ArchiveFindings`verwendet `detector/detectorId/findings/archive`
- `guardduty:GetMembers`verwendet `detector/detectorId/member/get`
- `guardduty:ListFindings`verwendet `detector/detectorId/findings` (kein Suffix)
- `guardduty:ListMembers`verwendet `detector/detectorId/member` (kein Suffix)

Die folgende Richtlinie gewährt Zuschüsse `guardduty:GetFindings` für einen bestimmten Detektor in der Region US-East-1 unter Verwendung des vollständigen Ressourcenpfads:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "guardduty:GetFindings",
    "Resource": "arn:aws:guardduty:us-
east-1:111122223333:detector/a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6/findings/get"
  }]
}
```

Verwenden von serviceverknüpften Rollen für Amazon GuardDuty

Amazon GuardDuty verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle (SLR) ist eine einzigartige Art von IAM-Rolle, mit der direkt verknüpft ist. GuardDuty Service-linked Rollen sind von vordefiniert GuardDuty und enthalten alle Berechtigungen, die GuardDuty erforderlich sind, um andere AWS Dienste in Ihrem Namen aufzurufen.

Mit einer serviceverknüpften Rolle können Sie sie einrichten, GuardDuty ohne die erforderlichen Berechtigungen manuell hinzufügen zu müssen. GuardDuty definiert die Berechtigungen der dienstbezogenen Rolle. Sofern die Berechtigungen nicht anders definiert sind, GuardDuty kann Only die Rolle übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

GuardDuty unterstützt die Verwendung von dienstbezogenen Rollen in allen Regionen, in denen diese Funktion verfügbar GuardDuty ist. Weitere Informationen finden Sie unter Regionen und Endpunkte.

Sie können die GuardDuty dienstverknüpfte Rolle erst löschen, nachdem Sie sie zuerst GuardDuty in allen Regionen deaktiviert haben, in denen sie aktiviert ist. Dadurch werden Ihre GuardDuty Ressourcen geschützt, da Sie die Zugriffsberechtigung nicht versehentlich entziehen können.

Informationen zu anderen Diensten, die dienstbezogene Rollen unterstützen, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren. Suchen Sie in der Spalte Rolle nach den Diensten, für die Ja steht. Service-Linked Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Service-linked Rollenberechtigungen für GuardDuty

GuardDuty verwendet die angegebene serviceverknüpfte Rolle (SLR). `AWSServiceRoleForAmazonGuardDuty` Die Spiegelreflexkamera ermöglicht GuardDuty die Ausführung der folgenden Aufgaben. Es ermöglicht auch GuardDuty , die abgerufenen Metadaten der EC2-Instance in die Erkenntnisse einzubeziehen, die sich GuardDuty möglicherweise über die potenzielle Bedrohung ergeben. Die serviceverknüpfte Rolle `AWSServiceRoleForAmazonGuardDuty` vertraut dem Service `guardduty.amazonaws.com`, sodass dieser die Rolle annehmen kann.

Die Berechtigungsrichtlinien helfen bei der GuardDuty Ausführung der folgenden Aufgaben:

- Verwenden Sie Amazon EC2 EC2-Aktionen, um Informationen über Ihre EC2-Instances, Images und Netzwerkkomponenten wie VPCs, Subnetze und Transit-Gateways zu verwalten und abzurufen.
- Verwenden Sie AWS Systems Manager Aktionen, um SSM-Verknüpfungen auf Amazon EC2-Instances zu verwalten, wenn Sie GuardDuty Runtime Monitoring mit automatisiertem Agenten für Amazon EC2 aktivieren. Wenn die GuardDuty automatische Agentenkonfiguration deaktiviert ist, werden nur die EC2-Instances GuardDuty berücksichtigt, die über ein Inclusion-Tag (:) verfügen. `GuardDutyManaged true`
- Verwenden Sie AWS Organizations Aktionen, um die zugehörigen Konten und die Organisations-ID zu beschreiben.
- Verwenden Sie Amazon-S3-Aktionen, um Informationen über S3-Buckets und Objekte abzurufen.
- Verwenden Sie AWS Lambda Aktionen, um Informationen über Ihre Lambda-Funktionen und -Tags abzurufen.
- Verwenden Sie Amazon-EKS-Aktionen, um Informationen über die EKS-Cluster zu verwalten und abzurufen und Amazon-EKS-Add-Ons auf EKS-Clustern zu verwalten. Die EKS-Aktionen rufen auch die Informationen über die zugehörigen Tags ab. GuardDuty
- Verwenden Sie IAM, um das zu erstellen, Service-linked Rollenberechtigungen für Malware Protection for EC2 nachdem Malware Protection for EC2 aktiviert wurde.
- Verwenden Sie Amazon ECS-Aktionen, um Informationen über die Amazon ECS-Cluster zu verwalten und abzurufen, Informationen über Aufgaben und Aufgabendefinitionen abzurufen und die Amazon ECS-Kontoeinstellungen mit zu verwalten`guarddutyActivate`. Die Aktionen im Zusammenhang mit Amazon ECS rufen auch die Informationen über die zugehörigen Tags ab. GuardDuty

Die Rolle ist mit der folgenden AWS -verwalteten Richtlinie namens `AmazonGuardDutyServiceRolePolicy` konfiguriert.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie AmazonGuardDutyServiceRolePolicyim Referenzhandbuch für AWS verwaltete Richtlinien.

Nachfolgend wird die der serviceverknüpften Rolle `AWSServiceRoleForAmazonGuardDuty` zugeordnete Vertrauensrichtlinie gezeigt:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Einzelheiten zu Aktualisierungen der `AmazonGuardDutyServiceRolePolicy` Richtlinie finden Sie unterGuardDuty Aktualisierungen der AWS verwalteten Richtlinien. Abonnieren Sie den RSS-Feed auf der Dokumentverlauf Seite, um automatische Benachrichtigungen über Änderungen an dieser Richtlinie zu erhalten.

Erstellen einer dienstbezogenen Rolle für GuardDuty

Die `AWSServiceRoleForAmazonGuardDuty` dienstverknüpfte Rolle wird automatisch erstellt, wenn Sie sie GuardDuty zum ersten Mal oder GuardDuty in einer unterstützten Region aktivieren, in der sie zuvor nicht aktiviert war. Sie können die serviceverknüpfte Rolle auch manuell mithilfe der IAM-Konsole, der oder der AWS CLI IAM-API erstellen.

> **Important**
>
> Die dienstverknüpfte Rolle, die für das GuardDuty delegierte Administratorkonto erstellt wurde, gilt nicht für die Mitgliedskonten. GuardDuty

Sie müssen Berechtigungen konfigurieren, damit ein IAM-Prinzipal (z. B. ein Benutzer, eine Gruppe oder eine Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Damit die `AWSServiceRoleForAmazonGuardDuty` dienstverknüpfte Rolle erfolgreich erstellt werden kann, muss der IAM-Prinzipal, den Sie GuardDuty mit verwenden, über die erforderlichen Berechtigungen verfügen. Um die erforderlichen Berechtigungen zu erteilen, weisen Sie diesem -Benutzer bzw. dieser-Gruppe oder -Rolle die folgende Richtlinie zu:

> **Note**
>
> Ersetzen Sie das Beispiel *`account ID`* im folgenden Beispiel durch Ihre tatsächliche AWS-Konto ID.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
            "Condition": {
                "StringLike": {
```

```
                    "iam:AWSServiceName": "guardduty.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
        }
    ]
}
```

Weitere Informationen zum Erstellen von IAM-Rollen finden Sie unter Erstellen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Bearbeitung einer serviceverknüpften Rolle für GuardDuty

GuardDuty erlaubt es Ihnen nicht, die `AWSServiceRoleForAmazonGuardDuty` dienstbezogene Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach der Erstellung einer serviceverknüpften Rolle nicht bearbeitet werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer dienstbezogenen Rolle für GuardDuty

Wenn Sie ein Feature oder einen Service, die bzw. der eine serviceverknüpfte Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte Entität, die nicht aktiv überwacht oder verwaltet wird.

> **Important**
>
> Wenn Sie Malware Protection for EC2 aktiviert haben, wird `AWSServiceRoleForAmazonGuardDuty` das Löschen nicht automatisch gelöscht. `AWSServiceRoleForAmazonGuardDutyMalwareProtection` Informationen zum Löschen `AWSServiceRoleForAmazonGuardDutyMalwareProtection` finden Sie unter Löschen einer serviceverknüpften Rolle für Malware Protection for EC2.

Sie müssen es zunächst GuardDuty in allen Regionen deaktivieren, in denen es aktiviert ist, um das zu löschen. `AWSServiceRoleForAmazonGuardDuty` Wenn der GuardDuty Dienst nicht deaktiviert ist, wenn Sie versuchen, die mit dem Dienst verknüpfte Rolle zu löschen, schlägt das Löschen fehl. Weitere Informationen finden Sie unter Aussetzen oder Deaktivieren GuardDuty.

Wenn Sie ihn deaktivieren GuardDuty, wird `AWSServiceRoleForAmazonGuardDuty` er nicht automatisch gelöscht. Wenn Sie es GuardDuty erneut aktivieren, wird das Bestehende verwendet`AWSServiceRoleForAmazonGuardDuty`.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die IAM-API AWS CLI, um die `AWSServiceRoleForAmazonGuardDuty` serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützt AWS-Regionen

Amazon GuardDuty unterstützt die Verwendung der `AWSServiceRoleForAmazonGuardDuty` serviceverknüpften Rolle überall AWS-Regionen dort, wo sie verfügbar GuardDuty ist. Eine Liste der Regionen, in denen GuardDuty das Produkt derzeit verfügbar ist, finden Sie unter GuardDuty Amazon-Endpunkte und Kontingente in der Allgemeine Amazon Web Services-Referenz.

Service-linked Rollenberechtigungen für Malware Protection for EC2

Malware Protection for EC2 verwendet die angegebene Service-Linked Role (SLR). `AWSServiceRoleForAmazonGuardDutyMalwareProtection` Diese Spiegelreflexkamera ermöglicht es Malware Protection for EC2, agentenlose Scans durchzuführen, um Malware in Ihrem Konto zu erkennen. GuardDuty Es ermöglicht GuardDuty die Erstellung eines EBS-Volume-Snapshots in Ihrem Konto und die gemeinsame Nutzung dieses Snapshots mit dem Dienstkonto. GuardDuty Nach der GuardDuty Auswertung des Snapshots werden die abgerufenen EC2-Instance- und Container-Workload-Metadaten in die Ergebnisse von Malware Protection for EC2 aufgenommen. Die serviceverknüpfte Rolle `AWSServiceRoleForAmazonGuardDutyMalwareProtection` vertraut dem Service `malware-protection.guardduty.amazonaws.com`, sodass dieser die Rolle annehmen kann.

Die Berechtigungsrichtlinien für diese Rolle helfen Malware Protection for EC2 dabei, die folgenden Aufgaben auszuführen:

- Verwenden Sie Amazon Elastic Compute Cloud (Amazon EC2) -Aktionen, um Informationen über Ihre Amazon EC2 EC2-Instances, Volumes und Snapshots abzurufen. Malware Protection for

EC2 gewährt auch die Erlaubnis, auf die Amazon EKS- und Amazon ECS-Cluster-Metadaten zuzugreifen.

- Erstellen Sie Snapshots für EBS-Volumes, bei denen das `GuardDutyExcluded`-Tag nicht auf `true` gesetzt ist. Standardmäßig werden die Snapshots mit einem `GuardDutyScanId`-Tag erstellt. Entfernen Sie dieses Tag nicht, da Malware Protection for EC2 sonst keinen Zugriff auf die Snapshots hat.

  > **Important**
  >
  > Wenn Sie das `GuardDutyExcluded` auf setzen`true`, kann der GuardDuty Dienst in future nicht mehr auf diese Snapshots zugreifen. Dies liegt daran, dass die anderen Anweisungen in dieser dienstbezogenen Rolle GuardDuty verhindern, dass Aktionen für die Snapshots ausgeführt werden, für die der Wert auf gesetzt ist. `GuardDutyExcluded` `true`

- Lassen Sie das Teilen und Löschen von Snapshots nur zu, wenn das `GuardDutyScanId`-Tag existiert und das `GuardDutyExcluded`-Tag nicht auf `true` gesetzt ist.

  > **Note**
  >
  > Lässt nicht zu, dass Malware Protection for EC2 die Snapshots veröffentlicht.

- Greifen Sie auf vom Kunden verwaltete Schlüssel zu, mit Ausnahme von Schlüsseln, für die ein `GuardDutyExcluded` Tag auf gesetzt ist`true`, `CreateGrant` um über den verschlüsselten Snapshot, der mit dem Dienstkonto geteilt wird, ein verschlüsseltes EBS-Volume zu erstellen und darauf zuzugreifen. GuardDuty Eine Liste der GuardDuty Dienstkonten für jede Region finden Sie unterGuardDuty Dienstkonten von AWS-Region.
- Greifen Sie auf CloudWatch Kundenprotokolle zu, um die Protokollgruppe Malware Protection for EC2 zu erstellen und die Malware-Scan-Ereignisprotokolle der `/aws/guardduty/malware-scan-events` Protokollgruppe zuzuordnen.
- Lassen Sie den Kunden entscheiden, ob er die Snapshots, auf denen Malware erkannt wurde, in seinem Konto behalten möchte. Wenn beim Scan Malware erkannt wird, ermöglicht GuardDuty die mit dem Service verknüpfte Rolle das Hinzufügen von zwei Tags zu Snapshots: und. `GuardDutyFindingDetected` `GuardDutyExcluded`

> **Note**
>
> Das `GuardDutyFindingDetected`-Tag gibt an, dass die Snapshots Malware enthalten.

- Ermitteln Sie, ob ein Volume mit einem von EBS verwalteten Schlüssel verschlüsselt ist. GuardDuty führt die `DescribeKey` Aktion zur Bestimmung `key Id` des EBS-managed Schlüssels in Ihrem Konto durch.
- Rufen Sie den Snapshot der EBS-Volumes, verschlüsselt mit Von AWS verwalteter Schlüssel, von Ihrem ab AWS-Konto und kopieren Sie ihn in den. GuardDuty Dienstkonto Zu diesem Zweck verwenden wir die Berechtigungen `GetSnapshotBlock` und. `ListSnapshotBlocks` GuardDuty scannt dann den Snapshot im Dienstkonto. Derzeit ist die Unterstützung von Malware Protection for EC2 zum Scannen von EBS-Volumes, die mit verschlüsselt sind, Von AWS verwalteter Schlüssel möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Region-specific Verfügbarkeit von Funktionen.
- Erlauben Sie Amazon EC2, AWS KMS im Namen von Malware Protection for EC2 anzurufen, um verschiedene kryptografische Aktionen mit vom Kunden verwalteten Schlüsseln durchzuführen. Aktionen wie `kms:ReEncryptTo` und `kms:ReEncryptFrom` sind erforderlich, um die Snapshots zu teilen, die mit den vom Kunden verwalteten Schlüsseln verschlüsselt sind. Es sind nur die Schlüssel zugänglich, für die das `GuardDutyExcluded`-Tag nicht auf `true` festgelegt ist.

Die Rolle ist mit der folgenden AWS -verwalteten Richtlinie namens `AmazonGuardDutyMalwareProtectionServiceRolePolicy` konfiguriert.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie AmazonGuardDutyMalwareProtectionServiceRolePolicyim Referenzhandbuch für AWS verwaltete Richtlinien.

Nachfolgend wird die der serviceverknüpften Rolle `AWSServiceRoleForAmazonGuardDutyMalwareProtection` zugeordnete Vertrauensrichtlinie gezeigt:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Eine dienstbezogene Rolle für Malware Protection for EC2 erstellen

Die `AWSServiceRoleForAmazonGuardDutyMalwareProtection` dienstbezogene Rolle wird automatisch erstellt, wenn Sie Malware Protection for EC2 zum ersten Mal aktivieren oder Malware Protection for EC2 in einer unterstützten Region aktivieren, in der Sie sie zuvor nicht aktiviert hatten. Sie können die serviceverknüpfte Rolle namens `AWSServiceRoleForAmazonGuardDutyMalwareProtection` auch manuell erstellen, indem Sie die IAM-Konsole, die CLI oder die IAM-API verwenden.

> **Note**
>
> Wenn Sie neu bei Amazon sind GuardDuty, ist Malware Protection for EC2 standardmäßig automatisch aktiviert.

> **Important**
>
> Die dienstbezogene Rolle, die für das delegierte GuardDuty Administratorkonto erstellt wurde, gilt nicht für die Mitgliedskonten. GuardDuty

Sie müssen Berechtigungen konfigurieren, damit ein IAM-Prinzipal (z. B. ein Benutzer, eine Gruppe oder eine Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Damit die `AWSServiceRoleForAmazonGuardDutyMalwareProtection` dienstverknüpfte Rolle erfolgreich erstellt werden kann, muss die IAM-Identität, die Sie GuardDuty mit verwenden, über die erforderlichen Berechtigungen verfügen. Um die erforderlichen Berechtigungen zu erteilen, weisen Sie diesem -Benutzer bzw. dieser-Gruppe oder -Rolle die folgende Richtlinie zu:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "guardduty:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": [
                        "malware-protection.guardduty.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:GetRole",
            "Resource": "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
        }
    ]
}
```

Weitere Informationen zum Erstellen von IAM-Rollen finden Sie unter Erstellen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Bearbeiten einer dienstbezogenen Rolle für Malware Protection for EC2

Mit Malware Protection for EC2 können Sie die dienstbezogene Rolle nicht bearbeiten. `AWSServiceRoleForAmazonGuardDutyMalwareProtection` Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach der Erstellung einer serviceverknüpften Rolle nicht bearbeitet werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer dienstbezogenen Rolle für Malware Protection for EC2

Wenn Sie ein Feature oder einen Service, die bzw. der eine serviceverknüpfte Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte Entität, die nicht aktiv überwacht oder verwaltet wird.

> **Important**
>
> Um den zu löschen`AWSServiceRoleForAmazonGuardDutyMalwareProtection`, müssen Sie zuerst den Malware-Schutz für EC2 in allen Regionen deaktivieren, in denen er aktiviert ist.
> Wenn Malware Protection for EC2 nicht deaktiviert ist, wenn Sie versuchen, die dienstbezogene Rolle zu löschen, schlägt der Löschvorgang fehl. Stellen Sie sicher, dass Sie zuerst Malware Protection for EC2 in Ihrem Konto deaktivieren.

Wenn Sie „Deaktivieren“ wählen, um den Dienst Malware Protection for EC2 zu beenden, `AWSServiceRoleForAmazonGuardDutyMalwareProtection` wird der Dienst nicht automatisch gelöscht. Wenn Sie dann „Aktivieren“ wählen, um den Dienst Malware Protection for EC2 erneut zu starten, GuardDuty wird der vorhandene Dienst wieder verwendet. `AWSServiceRoleForAmazonGuardDutyMalwareProtection`

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die AWS CLI oder die IAM-API, um die `AWSServiceRoleForAmazonGuardDutyMalwareProtection` serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützt AWS-Regionen

Amazon GuardDuty unterstützt die Verwendung der `AWSServiceRoleForAmazonGuardDutyMalwareProtection` serviceverknüpften Rolle in allen Bereichen, in AWS-Regionen denen Malware Protection for EC2 verfügbar ist.

Eine Liste der Regionen, in denen GuardDuty das Produkt derzeit verfügbar ist, finden Sie unter GuardDuty Amazon-Endpunkte und Kontingente in der Allgemeine Amazon Web Services-Referenz.

> **Note**
>
> Der Malware-Schutz für EC2 ist derzeit in AWS GovCloud (US-East) und AWS GovCloud (US-West) nicht verfügbar.

AWS verwaltete Richtlinien für Amazon GuardDuty

Um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen, ist es einfacher, AWS verwaltete Richtlinien zu verwenden, als Richtlinien selbst zu schreiben. Es erfordert Zeit und Fachwissen, um von Kunden verwaltete IAM-Richtlinien zu erstellen, die Ihrem Team nur die benötigten Berechtigungen bieten. Um schnell loszulegen, können Sie unsere AWS verwalteten Richtlinien verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS-Konto verfügbar. Weitere Informationen zu AWS verwalteten Richtlinien finden Sie im IAM-Benutzerhandbuch unter AWS Verwaltete Richtlinien.

AWS Dienste verwalten und aktualisieren AWS verwaltete Richtlinien. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Dienste fügen einer AWS verwalteten Richtlinie gelegentlich zusätzliche Berechtigungen hinzu, um neue Funktionen zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Es ist sehr wahrscheinlich, dass Dienste eine AWS verwaltete Richtlinie aktualisieren, wenn eine neue Funktion eingeführt wird oder wenn neue Operationen verfügbar werden. Dienste entfernen keine Berechtigungen aus einer AWS verwalteten Richtlinie, sodass durch Richtlinienaktualisierungen Ihre bestehenden Berechtigungen nicht beeinträchtigt werden.

AWS Unterstützt außerdem verwaltete Richtlinien für Jobfunktionen, die sich über mehrere Dienste erstrecken. Die ReadOnlyAccess AWS verwaltete Richtlinie bietet beispielsweise schreibgeschützten Zugriff auf alle AWS Dienste und Ressourcen. Wenn ein Dienst eine neue Funktion startet, werden nur Leseberechtigungen für neue Operationen und Ressourcen AWS hinzugefügt. Eine Liste und

Beschreibungen der Richtlinien für Auftragsfunktionen finden Sie in Verwaltete AWS -Richtlinien für Auftragsfunktionen im IAM-Leitfaden.

Die `Version`-Richtlinienelemente legen die Sprachsyntaxregeln fest, die für die Verarbeitung einer Richtlinie verwendet werden sollen. Die folgenden Richtlinien beinhalten die aktuelle Version, die IAM unterstützt. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Version.

AWS verwaltete Richtlinie: AmazonGuardDutyFullAccess_v2 (empfohlen)

Sie können die AmazonGuardDutyFullAccess_v2-Richtlinie an Ihre IAM-Identitäten anfügen. Diese Richtlinie gewährt einem Benutzer vollen Zugriff, um alle GuardDuty Aktionen auszuführen und auf die erforderlichen Ressourcen zuzugreifen. Zwischen AmazonGuardDutyFullAccess_v2 und GuardDuty empfiehlt das Anhängen AmazonGuardDutyFullAccess, AmazonGuardDutyFullAccess_v2 da es mehr Sicherheit bietet und Verwaltungsaktionen auf GuardDuty Dienstprinzipale beschränkt.

Berechtigungsdetails

Die AmazonGuardDutyFullAccess_v2 Richtlinie umfasst die folgenden Berechtigungen:

- `GuardDuty`— Ermöglicht Benutzern vollen Zugriff auf alle GuardDuty Aktionen.
- `IAM`:
  - Ermöglicht Benutzern, eine GuardDuty dienstbezogene Rolle zu erstellen.
  - Ermöglicht das Anzeigen und Verwalten von IAM-Rollen und deren Richtlinien für. GuardDuty
  - Ermöglicht Benutzern, eine Rolle an zu GuardDuty übergeben. GuardDuty verwendet diese Rolle, um den Malware-Schutz für S3 zu aktivieren und S3-Objekte auf Malware zu scannen. GuardDuty verwendet diese Rolle auch, um Scans für Malware Protection for AWS Backup zu initiieren.
  - Die Berechtigung zum Ausführen einer `iam:GetRole` Aktion für `AWSServiceRoleForAmazonGuardDutyMalwareProtection` legt fest, ob die serviceverknüpfte Rolle (SLR) für Malware Protection for EC2 in einem Konto vorhanden ist.
- `Organizations`:
  - Erlaubt Benutzern das Lesen (Anzeigen) der GuardDuty Organisationsstruktur und der Konten.
  - Ermöglicht Benutzern, einen delegierten Administrator zu benennen und Mitglieder für eine GuardDuty Organisation zu verwalten.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AmazonGuardDutyFullAccess_v2 im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: AmazonGuardDutyFullAccess

Sie können die `AmazonGuardDutyFullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

> **Important**
>
> Für mehr Sicherheit und eingeschränkte Berechtigungen für GuardDuty Dienstprinzipale empfehlen wir Ihnen die Verwendung AWS verwaltete Richtlinie: AmazonGuardDutyFullAccess_v2 (empfohlen) von.

Diese Richtlinie gewährt Administratorberechtigungen, die einem Benutzer vollen Zugriff auf alle GuardDuty Aktionen und Ressourcen gewähren.

Berechtigungsdetails

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `GuardDuty`— Ermöglicht Benutzern vollen Zugriff auf alle GuardDuty Aktionen.
- `IAM`:
  - Ermöglicht Benutzern, die GuardDuty dienstbezogene Rolle zu erstellen.
  - Ermöglicht einem Administratorkonto die Aktivierung GuardDuty für Mitgliedskonten.
  - Ermöglicht Benutzern, eine Rolle an zu übergeben GuardDuty. GuardDuty verwendet diese Rolle, um den Malware-Schutz für S3 zu aktivieren und S3-Objekte auf Malware zu scannen. GuardDuty verwendet diese Rolle auch, um Scans für Malware Protection for AWS Backup zu initiieren.
- `Organizations`— Ermöglicht Benutzern, einen delegierten Administrator zu benennen und Mitglieder für eine GuardDuty Organisation zu verwalten.

Mit der Berechtigung zum Ausführen einer `iam:GetRole` Aktion `AWSServiceRoleForAmazonGuardDutyMalwareProtection` wird festgelegt, ob die serviceverknüpfte Rolle (SLR) für Malware Protection for EC2 in einem Konto vorhanden ist.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie AmazonGuardDutyFullAccessim Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: AmazonGuardDutyReadOnlyAccess

Sie können die `AmazonGuardDutyReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Benutzern nur Leseberechtigungen, die es Benutzern ermöglichen, GuardDuty Ergebnisse und Details Ihrer GuardDuty Organisation einzusehen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `GuardDuty`— Ermöglicht Benutzern, GuardDuty Ergebnisse einzusehen und API-Operationen durchzuführen, die mit `GetList`, oder beginnen. `Describe`
- `Organizations`— Ermöglicht Benutzern das Abrufen von Informationen über Ihre GuardDuty Organisationskonfiguration, einschließlich Details zum delegierten Administratorkonto.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie AmazonGuardDutyReadOnlyAccessim Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: AmazonGuardDutyServiceRolePolicy

Sie können `AmazonGuardDutyServiceRolePolicy` nicht an Ihre IAM-Entitäten anhängen. Diese AWS verwaltete Richtlinie ist einer dienstbezogenen Rolle zugeordnet, mit der GuardDuty Sie Aktionen in Ihrem Namen ausführen können. Weitere Informationen finden Sie unter Service-linked Rollenberechtigungen für GuardDuty.

GuardDuty Aktualisierungen der AWS verwalteten Richtlinien

Hier finden Sie Informationen zu Aktualisierungen AWS verwalteter Richtlinien, die GuardDuty seit Beginn der Nachverfolgung dieser Änderungen durch diesen Dienst vorgenommen wurden. Abonnieren Sie den RSS-Feed auf der Seite GuardDuty Dokumentenverlauf, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten.

Änderungen	Beschreibung	Datum
AmazonGuardDutyServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Es wurden `s3:ListBucket` Berechtigungen zum Abrufen von `ecs:DescribeTaskDefinition` S3-Bucket-Auflistungen `ecs:DescribeTasks` und Berechtigungen zum Abrufen von Informationen über Amazon ECS-Aufgaben und Aufgabendefinitionen hinzugefügt.	23. April 2026

AmazonGuardDutyServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Es wurde die `cloudtrail:CreateServiceLinkedChannel` Erlaubnis hinzugefügt, einen zusätzlichen Mechanismus für die Nutzung von AWS CloudTrail Ereignissen zu aktivieren.
	
	`{`
	`"Sid": "CloudTrailCreateServiceLinkedChannelSid",`
	`"Effect": "Allow",`
	`"Action": [`
	`"cloudtrail:CreateServiceLinkedChannel"`
	`],`
		25. März 2026

Änderungen	Beschreibung	Datum
	"Resource": "arn:aws:cloudtrail:*:*:channel/aws-service-channel/guardduty/*", "Condition": { "StringEquals": { "aws:ResourceAccount": "${aws:PrincipalAccount}" } } }	

Änderungen	Beschreibung	Datum
`AmazonGuardDutyFullAccess` – als veraltet gekennzeichnet	Diese Richtlinie wurde durch eine eingeschränkte Richtlinie namens `AmazonGuardDutyFullAccess_v2` ersetzt. Nach dem 13. März 2026 können Sie die `AmazonGuardDutyFullAccess` Richtlinie keinen neuen Benutzern, Gruppen oder Rollen zuordnen. Weitere Informationen finden Sie unter AWS verwaltete Richtlinie: AmazonGuardDutyFullAccess_v2 (empfohlen).	13. März 2026

Änderungen	Beschreibung	Datum

AmazonGuardDutyFullAccess_v2 – Aktualisierung auf eine bestehende Richtlinie	Es wurde eine Berechtigung hinzugefügt, mit der Sie eine IAM-Rolle übergeben können, GuardDuty wenn Sie Malware Protection for AWS Backup aktivieren.
	
	{
	"Sid": "AllowPassRoleToMalwareProtection",
	"Effect": "Allow",
	"Action": [
	"iam:PassRole"
	],
	"Resource": "arn:aws:iam::*:role/*",
	"Condition": {
	"StringEquals": {
	"iam:PassedToService": [
	"malware-protectio
		19. November 2025

Änderungen	Beschreibung	Datum
	n-plan.guardduty.amazonaws.com", "malware-protection.guardduty.amazonaws.com"] } } }	

Änderungen	Beschreibung	Datum

AmazonGuardDutyFullAccess – Aktualisierung auf eine bestehende Richtlinie	Es wurde eine Berechtigung hinzugefügt, mit der Sie eine IAM-Rolle übergeben können, GuardDuty wenn Sie Malware Protection for AWS Backup aktivieren.
	
	{
	"Sid": "AllowPassRoleToMalwareProtection",
	"Effect": "Allow",
	"Action": [
	"iam:PassRole"
	],
	"Resource": "arn:aws:iam::*:role/*",
	"Condition": {
	"StringEquals": {
	"iam:PassedToService": [
	"malware-protectio
		19. November 2025

Änderungen	Beschreibung	Datum
	n-plan.guardduty.amazonaws.com", "malware-protection.guardduty.amazonaws.com"] } } }	
AmazonGuardDutyFullAccess_v2— Eine neue Richtlinie wurde hinzugefügt	Eine neue AmazonGuardDutyFullAccess_v2 Richtlinie wurde hinzugefügt. Dies wird empfohlen, da ihre Berechtigungen die Sicherheit erhöhen, indem sie die administrativen Aktionen auf die GuardDuty Dienstprinzipale beschränken, die auf IAM-Rollen und -Richtlinien sowie auf der Integration basieren. AWS Organizations	04. Juni 2025
AmazonGuardDutyServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Die `ec2:DescribeVpcs` Erlaubnis wurde hinzugefügt. Auf diese Weise können GuardDuty VPC-Updates nachverfolgt werden, z. B. das Abrufen des VPC-CIDR.	22. August 2024

Änderungen	Beschreibung	Datum
AmazonGuardDutyFullAccess – Aktualisierung auf eine bestehende Richtlinie	Es wurde eine Berechtigung hinzugefügt, mit der Sie eine IAM-Rolle übergeben können, GuardDuty wenn Sie Malware Protection for S3 aktivieren. `{ "Sid": "AllowPassRoleToMalwareProtectionPlan", "Effect": "Allow", "Action": [ "iam:PassRole" ], "Resource": "arn:aws:iam::*:role/*", "Condition": { "StringEquals": { "iam:PassedToService": "malware-protection-plan.guardduty.amazonaws.com" } } }`	10. Juni 2024

Änderungen	Beschreibung	Datum
AmazonGuardDutyServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie.	Verwenden Sie AWS Systems Manager Aktionen, um SSM-Verknüpfungen auf Amazon EC2-Instances zu verwalten, wenn Sie GuardDuty Runtime Monitoring mit automatisiertem Agenten für Amazon EC2 aktivieren. Wenn die GuardDuty automatische Agentenkonfiguration deaktiviert ist, werden nur die EC2-Instances GuardDuty berücksichtigt, die über ein Inclusion-Tag (:) verfügen. `GuardDutyManaged true`	26. März 2024
AmazonGuardDutyServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie.	GuardDuty hat eine neue Berechtigung hinzugefügt`organization:DescribeOrganization` , um die Organisations-ID des gemeinsamen Amazon VPC-Kontos abzurufen und die Amazon VPC-Endpunktrichtlinie mit der Organisations-ID festzulegen.	9. Februar 2024

Änderungen	Beschreibung	Datum
AmazonGuardDutyMalwareProtectionServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie.	Malware Protection for EC2 hat zwei zusätzliche Berechtigungen hinzugefügt: `GetSnapshotBlock` Sie `ListSnapshotBlocks` können den Snapshot eines EBS-Volumes (verschlüsselt mit Von AWS verwalteter Schlüssel) von Ihrem abrufen AWS-Konto und in das GuardDuty Dienstkonto kopieren, bevor der Malware-Scan gestartet wird.	25. Januar 2024
AmazonGuardDutyServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Neue Berechtigungen wurden hinzugefügt, um das Hinzufügen von `guardduty Activate` Amazon ECS-Kontoeinstellungen und das Ausführen von Listen- und Beschreibungsvorgängen auf Amazon ECS-Clustern zu ermöglichen GuardDuty .	26. November 2023
AmazonGuardDutyReadOnlyAccess – Aktualisierung auf eine bestehende Richtlinie	GuardDuty hat eine neue Richtlinie für `organizations` to hinzugefügt `ListAccounts` .	16. November 2023
AmazonGuardDutyFullAccess – Aktualisierung auf eine bestehende Richtlinie	GuardDuty hat eine neue Richtlinie für `organizations` to hinzugefügt `ListAccounts` .	16. November 2023

Änderungen	Beschreibung	Datum
AmazonGuardDutyServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	GuardDuty neue Berechtigungen hinzugefügt, um die kommende GuardDuty EKS Runtime Monitoring-Funktion zu unterstützen.	08. März 2023
AmazonGuardDutyServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	GuardDuty hat neue Berechtigungen hinzugefügt, um das Erstellen GuardDuty einer Service-linked Rolle für Malware Protection for EC2 zu ermöglichen. Dies wird dazu beitragen, den Prozess der Aktivierung von Malware Protection for EC2 zu GuardDuty optimieren. GuardDuty kann jetzt die folgende IAM-Aktion ausführen: `{ "Effect": "Allow", "Action": "iam:CreateServiceLinkedRole", "Resource": "*", "Condition": { "StringEquals": { "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com" } } }`	21. Februar 2023

Änderungen	Beschreibung	Datum
AmazonGuardDutyFullAccess – Aktualisierung auf eine bestehende Richtlinie	GuardDuty ARN für `iam:GetRole` to aktualisiert*`AWSServiceRoleForAmazonGuardDutyMalwareProtection` .	26. Juli 2022
AmazonGuardDutyFullAccess – Aktualisierung auf eine bestehende Richtlinie	GuardDuty hat eine neue hinzugefügt`AWSServiceName` , um die Erstellung einer dienstbezogenen Rolle mithilfe des GuardDuty Malware Protection `iam:CreateServiceLinkedRole` for EC2-Dienstes zu ermöglichen. GuardDuty kann jetzt die `iam:GetRole` Aktion ausführen, für die Informationen abgerufen werden sollen. `AWSServiceRole`	26. Juli 2022

Änderungen	Beschreibung	Datum
AmazonGuardDutyServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	GuardDuty neue Berechtigungen hinzugefügt, um die Verwendung von Amazon EC2 EC2-Netzwerkaktionen zur Verbesserung der Ergebnisse zu ermöglichen GuardDuty . GuardDuty kann jetzt die folgenden EC2-Aktionen ausführen, um Informationen darüber zu erhalten, wie Ihre EC2-Instances kommunizieren. Diese Informationen werden verwendet, um die Genauigkeit der Erkenntnisse zu verbessern. • `ec2:DescribeVpcEndpoints` • `ec2:DescribeSubnets` • `ec2:DescribeVpcPeeringConnections` • `ec2:DescribeTransitGatewayAttachments`	3. August 2021
GuardDuty hat begonnen, Änderungen zu verfolgen	GuardDuty hat begonnen, Änderungen für die AWS verwalteten Richtlinien zu verfolgen.	3. August 2021

Fehlerbehebung Amazon GuardDuty Amazon-Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit GuardDuty IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion durchzuführen in GuardDuty
- Ich bin nicht berechtigt, iam: PassRole auszuführen.
- Ich möchte Personen außerhalb meiner Umgebung zulassen AWS-Konto um auf meine GuardDuty Ressourcen zuzugreifen.

Ich bin nicht berechtigt, eine Aktion durchzuführen in GuardDuty

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven *`my-example-widget`*-Ressource anzuzeigen, jedoch nicht über `guardduty:`*`GetWidget`*-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 guardduty:GetWidget on resource: my-example-widget
```

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `guardduty:`*`GetWidget`*-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam: PassRole auszuführen.

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zum Durchführen der `iam:PassRole`-Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an GuardDuty übergeben zu können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in GuardDuty auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb meiner Umgebung zulassen AWS-Konto um auf meine GuardDuty Ressourcen zuzugreifen.

Sie können eine Rolle erstellen, mit der Benutzer mit anderen Konten oder Personen außerhalb Ihrer Organisation auf Ihre Ressourcen zugreifen können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob diese Funktionen GuardDuty unterstützt werden, finden Sie unterSo GuardDuty arbeitet Amazon mit IAM.
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Konformitätsüberprüfung für Amazon GuardDuty

Unser neues AWS Anmeldeerlebnis ist nicht für regulierte Workloads konzipiert. Wenn Sie unser neues AWS Anmeldeerlebnis nutzen, es aber AWS für regulierte Workloads nutzen möchten, können Sie sich für erweiterte Funktionen für AWS Ihre Umgebung anmelden oder diese aktivieren. AWS

Um zu erfahren, ob AWS-Service ein Programm AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm und wählen Sie das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme, .

Sie können Auditberichte von Drittanbietern mit herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen im Abschnitt Berichte AWS Artifact .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens sowie den geltenden Gesetzen und Vorschriften ab. Weitere Informationen zu Ihrer Compliance-Verantwortung bei der Verwendung AWS-Services finden Sie in der AWS Sicherheitsdokumentation.

Resilienz bei Amazon GuardDuty

Die AWS globale Infrastruktur basiert auf AWS Regionen und Availability Zones. Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die über hoch redundante Netzwerke mit niedriger Latenz und hohen Durchsätzen verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu AWS Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Infrastruktursicherheit bei Amazon GuardDuty

Als verwalteter Service GuardDuty ist Amazon durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe für den Zugriff GuardDuty über das Netzwerk. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Cipher-Suites mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Amazon GuardDuty - und Schnittstellen-VPC-Endpunkte ()AWS PrivateLink

Sie können eine private Verbindung zwischen Ihrer VPC und Amazon herstellen, GuardDuty indem Sie einen VPC-Schnittstellen-Endpunkt erstellen. Schnittstellenendpunkte basieren auf einer Technologie AWS PrivateLink, mit der Sie privat auf GuardDuty APIs zugreifen können, ohne dass ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder eine AWS Direct Connect-Verbindung erforderlich ist. Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um mit GuardDuty APIs zu kommunizieren. Datenverkehr zwischen Ihrer VPC und GuardDuty verlässt das Amazon-Netzwerk nicht.

Jeder Schnittstellenendpunkt wird durch eine oder mehrere Elastic-Network-Schnittstellen in Ihren Subnetzen dargestellt.

Weitere Informationen finden Sie im Handbuch unter Interface VPC endpoints (AWS PrivateLink).AWS PrivateLink

Überlegungen zu GuardDuty VPC-Endpunkten

Bevor Sie einen Schnittstellen-VPC-Endpunkt für einrichten, stellen Sie sicher GuardDuty, dass Sie die Eigenschaften und Einschränkungen der Schnittstellenendpunkte im AWS PrivateLink Handbuch lesen.

GuardDuty unterstützt Aufrufe aller API-Aktionen von Ihrer VPC aus.

Erstellen eines Schnittstellen-VPC-Endpunkts für GuardDuty

Sie können einen VPC-Endpunkt für den GuardDuty Service entweder mit der Amazon VPC-Konsole oder mit AWS Command Line Interface ()AWS CLI erstellen. Weitere Informationen finden Sie unter Erstellen eines Schnittstellenendpunkts im AWS PrivateLink -Leitfaden.

Erstellen Sie einen VPC-Endpunkt für die GuardDuty Verwendung des folgenden Dienstnamens:

- com.amazonaws. *region*. Wachdienst
- com.amazonaws. *region*.guardduty-fips (FIPS-Endpunkt)

Wenn Sie privates DNS für den Endpunkt aktivieren, können Sie API-Anfragen an die GuardDuty Verwendung des Standard-DNS-Namens für die Region stellen, z. B. `guardduty.us-east-1.amazonaws.com`

Weitere Informationen finden Sie im AWS PrivateLink Handbuch unter Zugreifen auf einen Dienst über einen Schnittstellenendpunkt.

Erstellen einer VPC-Endpunktrichtlinie für GuardDuty

Sie können eine Endpunktrichtlinie an Ihren VPC-Endpunkt anhängen, der den Zugriff auf GuardDuty steuert. Die Richtlinie gibt die folgenden Informationen an:

- Prinzipal, der die Aktionen ausführen kann.
- Aktionen, die ausgeführt werden können
- Die Ressourcen, für die Aktionen ausgeführt werden können.

Weitere Informationen finden Sie im Handbuch unter Steuern des Zugriffs auf Dienste mit VPC-Endpunkten.AWS PrivateLink

Beispiel: VPC-Endpunktrichtlinie für Aktionen GuardDuty

Im Folgenden finden Sie ein Beispiel für eine Endpunktrichtlinie für GuardDuty. Wenn diese Richtlinie an einen Endpunkt angehängt ist, gewährt sie allen Prinzipalen auf allen Ressourcen Zugriff auf die aufgelisteten GuardDuty Aktionen.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "guardduty:listDetectors",
            "guardduty:getDetector",
```

```
            "guardduty:getFindings"
         ],
         "Resource":"*"
      }
   ]
}
```

Gemeinsam genutzte Subnetze

Sie können VPC-Endpunkte in Subnetzen, die mit Ihnen geteilt werden, nicht erstellen, beschreiben, ändern oder löschen. Sie können die VPC-Endpunkte jedoch in Subnetzen verwenden, die mit Ihnen geteilt werden. Weitere Informationen zur Freigabe von VPCs finden Sie unter Freigeben Ihrer VPC für andere Konten im Amazon-VPC-Benutzerhandbuch.

GuardDuty Integration mit AWS Sicherheitsdiensten

GuardDuty kann in andere AWS Sicherheitsdienste integriert werden. Diese Dienste können Daten aufnehmen GuardDuty , sodass Sie die Ergebnisse auf neue Weise betrachten können. Sehen Sie sich die folgenden Integrationsoptionen an, um mehr darüber zu erfahren, wie dieser Dienst für die Verwendung eingerichtet ist. GuardDuty

Integration GuardDuty mit AWS Security Hub CSPM

AWS Security Hub CSPM sammelt Sicherheitsdaten aus all Ihren AWS Konten, Diensten und unterstützten Produkten von Drittanbietern, um den Sicherheitsstatus Ihrer Umgebung gemäß Industriestandards und Best Practices zu bewerten. Security Hub CSPM bewertet nicht nur Ihren Sicherheitsstatus, sondern bietet auch einen zentralen Ort für Erkenntnisse aus all Ihren integrierten AWS Services und AWS Partnerprodukten. Wenn Sie Security Hub CSPM mit aktivieren, können die GuardDuty Ergebnisdaten GuardDuty automatisch von Security Hub CSPM aufgenommen werden.

Weitere Informationen zur Verwendung von Security Hub CSPM finden Sie unter GuardDuty . Integration in AWS Security Hub CSPM

Integration GuardDuty mit Amazon Detective

Amazon Detective verwendet Protokolldaten aus all Ihren AWS Konten, um Datenvisualisierungen für Ihre Ressourcen und IP-Adressen zu erstellen, die mit Ihrer Umgebung interagieren. Die Visualisierungen von Detective helfen Ihnen dabei, Sicherheitsprobleme schnell und einfach zu untersuchen. Sobald beide Dienste aktiviert sind, können Sie von der GuardDuty Suche nach Details zu Informationen in der Detective-Konsole wechseln.

Weitere Informationen zur Verwendung von Detective mit GuardDuty finden Sie unterIntegration mit Amazon Detective.

Integration in AWS Security Hub CSPM

AWS Security Hub CSPM liefert einen umfassenden Überblick über den Sicherheitsstatus in AWS und hilft Ihnen dabei, Ihre Umgebung anhand von Sicherheitsstandards und bewährten Methoden der Branche zu überprüfen. Security Hub CSPM sammelt Sicherheitsdaten von AWS Konten, Diensten und unterstützten Partnerprodukten von Drittanbietern und hilft Ihnen dabei, Ihre Sicherheitstrends zu analysieren und die Sicherheitsprobleme mit der höchsten Priorität zu identifizieren.

Die GuardDuty Amazon-Integration mit Security Hub CSPM ermöglicht es Ihnen, Ergebnisse von an Security Hub CSPM GuardDuty zu senden. Security Hub CSPM kann diese Ergebnisse dann in die Analyse Ihres Sicherheitsstatus einbeziehen.

Inhalt

- So GuardDuty sendet Amazon Ergebnisse an AWS Security Hub CSPM
  - Arten von Ergebnissen, die GuardDuty an Security Hub CSPM gesendet werden
    - Latenz beim Senden neuer Ergebnisse
    - Wiederholter Versuch, wenn Security Hub CSPM nicht verfügbar ist
    - Aktualisieren von vorhandenen Erkenntnissen in Security Hub CSPM
- Ergebnisse anzeigen in GuardDuty AWS Security Hub CSPM
  - Interpretieren von GuardDuty Fundnamen in AWS Security Hub CSPM
  - Typischer Befund von GuardDuty
- Aktivieren und Konfigurieren der Integration
- Verwendung von GuardDuty Steuerelementen in Security Hub CSPM
- Einstellung der Veröffentlichung der Ergebnisse im Security Hub CSPM

So GuardDuty sendet Amazon Ergebnisse an AWS Security Hub CSPM

AWS Security Hub CSPM In werden Sicherheitsprobleme als Ergebnisse erfasst. Einige Ergebnisse stammen aus Problemen, die von anderen AWS Diensten oder von Drittanbietern entdeckt wurden. Security Hub CSPM verfügt außerdem über eine Reihe von Regeln, anhand derer Sicherheitsprobleme erkannt und Ergebnisse generiert werden.

Security Hub CSPM bietet Tools zur Verwaltung von Erkenntnissen aus all diesen Quellen. Sie können Listen mit Erkenntnissen anzeigen und filtern und Details zu einer Erkenntnis anzeigen. Weitere Informationen finden Sie unter Anzeigen der Erkenntnisse im AWS Security Hub -Benutzerhandbuch. Sie können auch den Status einer Untersuchung zu einer Erkenntnis nachverfolgen. Weitere Informationen finden Sie unter Ergreifen von Maßnahmen zu Erkenntnissen im AWS Security Hub -Benutzerhandbuch.

Alle Ergebnisse in Security Hub CSPM verwenden ein standardmäßiges JSON-Format, das AWS Security Finding Format (ASFF). Das ASFF enthält Details über die Ursache des Problems, die betroffenen Ressourcen und den aktuellen Status der Erkenntnis. Siehe AWS -Security Finding-Format (ASFF) im AWS Security Hub -Leitfaden.

Amazon GuardDuty ist einer der AWS Dienste, der Ergebnisse an Security Hub CSPM sendet.

Arten von Ergebnissen, die GuardDuty an Security Hub CSPM gesendet werden

Sobald Sie Security Hub CSPM für dasselbe Konto innerhalb desselben aktiviert GuardDuty haben AWS-Region, GuardDuty werden alle generierten Ergebnisse an Security Hub CSPM gesendet. Diese Ergebnisse werden mit dem Security Finding Format (ASFF) an AWS Security Hub CSPM gesendet. In ASFF gibt das `Types`-Feld die Art der Erkenntnis an.

Latenz beim Senden neuer Ergebnisse

Wenn ein neues Ergebnis GuardDuty erstellt wird, wird es normalerweise innerhalb von fünf Minuten an Security Hub CSPM gesendet.

Wiederholter Versuch, wenn Security Hub CSPM nicht verfügbar ist

Wenn Security Hub CSPM nicht verfügbar ist, GuardDuty versucht es erneut, die Ergebnisse zu senden, bis sie empfangen werden.

Aktualisieren von vorhandenen Erkenntnissen in Security Hub CSPM

Nachdem es ein Ergebnis an Security Hub CSPM gesendet hat, GuardDuty sendet es Updates, um zusätzliche Beobachtungen der Findungsaktivität zu berücksichtigen, an Security Hub CSPM. Die neuen Beobachtungen dieser Ergebnisse werden basierend auf den Schritt 5 — Häufigkeit für den Export von Ergebnissen Einstellungen in Ihrem an Security Hub CSPM gesendet. AWS-Konto

Wenn Sie einen Befund archivieren oder die Archivierung aufheben, GuardDuty wird dieser Befund nicht an Security Hub CSPM gesendet. Alle manuell dearchivierten Ergebnisse, die später aktiv werden, werden nicht an Security Hub CSPM gesendet. GuardDuty

Ergebnisse anzeigen in GuardDuty AWS Security Hub CSPM

Melden Sie sich bei an AWS-Managementkonsole und öffnen Sie die AWS Security Hub CSPM Konsole unter https://console.aws.amazon.com/securityhub/.

Sie können jetzt eine der folgenden Methoden verwenden, um die GuardDuty Ergebnisse in der Security Hub CSPM-Konsole anzuzeigen:

Option 1: Integrationen in Security Hub CSPM verwenden

1. Wählen Sie im linken Navigationsbereich Integrationen aus.
2. Überprüfen Sie auf der Seite Integrationen den Status für Amazon: GuardDuty.

- Wenn der Status „Ergebnisse werden akzeptiert“ lautet, wählen Sie neben „Ergebnisse akzeptieren“ die Option Ergebnisse anzeigen aus.
- Falls nicht, finden Sie weitere Informationen zur Funktionsweise von Integrationen unter Security Hub CSPM-Integrationen im Benutzerhandbuch.AWS Security Hub

Option 2: Ergebnisse im Security Hub CSPM verwenden

1. Wählen Sie im linken Navigationsbereich Findings aus.
2. Fügen Sie auf der Seite Ergebnisse den Filter Produktname hinzu und geben Sie ein**`GuardDuty`**, um nur GuardDuty Ergebnisse anzuzeigen.

Interpretieren von GuardDuty Fundnamen in AWS Security Hub CSPM

GuardDuty sendet die Ergebnisse mithilfe des Security Finding Formats (ASFF) an AWS Security Hub CSPM. In ASFF gibt das `Types`-Feld die Art der Erkenntnis an. ASFF-Typen verwenden ein anderes Benennungsschema als Typen. GuardDuty In der folgenden Tabelle sind alle GuardDuty Findetypen mit ihren ASFF-Gegenstücken aufgeführt, so wie sie in Security Hub CSPM erscheinen.

> **Note**
>
> Für einige GuardDuty Ergebnisarten weist Security Hub CSPM unterschiedliche ASFF-Suchnamen zu, je nachdem, ob die Ressourcenrolle des Ergebnisdetails ACTOR oder TARGET war. Weitere Informationen finden Sie unter Erkenntnisdetails.

GuardDuty Findetyp	ASFF-Ergebnistyp
AttackSequence:IAM/CompromisedCredentials	TTPs/AttackSequence:IAM/CompromisedCredentials
AttackSequence:S3/CompromisedData	TTPs/AttackSequence:S3/CompromisedData
Backdoor:EC2/C&CActivity.B	TTPs/Command and Control/Backdoor:EC2-C&CActivity.B
Backdoor:EC2/C&CActivity.B!DNS	TTPs/Command and Control/Backdoor:EC2-C&CActivity.B!DNS

GuardDuty Findetyp	ASFF-Ergebnistyp
Backdoor:EC2/DenialOfService.Dns	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Dns
Backdoor:EC2/DenialOfService.Tcp	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Tcp
Backdoor:EC2/DenialOfService.Udp	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Udp
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	TTPs/Command and Control/Backdoor:EC2-DenialOfService.UdpOnTcpPorts
Backdoor:EC2/DenialOfService.UnusualProtocol	TTPs/Command and Control/Backdoor:EC2-DenialOfService.UnusualProtocol
Backdoor:EC2/Spambot	TTPs/Command and Control/Backdoor:EC2-Spambot
Behavior:EC2/NetworkPortUnusual	Unusual Behaviors/VM/Behavior:EC2-NetworkPortUnusual
Behavior:EC2/TrafficVolumeUnusual	Unusual Behaviors/VM/Behavior:EC2-TrafficVolumeUnusual
Backdoor:Lambda/C&CActivity.B	TTPs/Command and Control/Backdoor:Lambda-C&CActivity.B
Backdoor:Runtime/C&CActivity.B	TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B
Backdoor:Runtime/C&CActivity.B!DNS	TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B!DNS
CredentialAccess:IAMUser/AnomalousBehavior	TTPs/Credential Access/IAMUser-AnomalousBehavior
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	TTPs/AnomalousBehavior/CredentialAccess:Kubernetes-SecretsAccessed

GuardDuty Findetyp	ASFF-Ergebnistyp
CredentialAccess:Kubernetes/MaliciousIPCaller	TTPs/CredentialAccess/CredentialAccess:Kubernetes-MaliciousIPCaller
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	TTPs/CredentialAccess/CredentialAccess:Kubernetes-MaliciousIPCaller.Custom
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	TTPs/CredentialAccess/CredentialAccess:Kubernetes-SuccessfulAnonymousAccess
CredentialAccess:Kubernetes/TorIPCaller	TTPs/CredentialAccess/CredentialAccess:Kubernetes-TorIPCaller
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	TTPs/Credential Access/CredentialAccess:RDS-AnomalousBehavior.FailedLogin
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	TTPs/Credential Access/CredentialAccess:RDS-AnomalousBehavior.SuccessfulBruteForce
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	TTPs/Credential Access/CredentialAccess:RDS-AnomalousBehavior.SuccessfulLogin
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	TTPs/Credential Access/CredentialAccess:RDS-MaliciousIPCaller.FailedLogin
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	TTPs/Credential Access/CredentialAccess:RDS-MaliciousIPCaller.SuccessfulLogin
CredentialAccess:RDS/TorIPCaller.FailedLogin	TTPs/Credential Access/CredentialAccess:RDS-TorIPCaller.FailedLogin
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	TTPs/Credential Access/CredentialAccess:RDS-TorIPCaller.SuccessfulLogin
CryptoCurrency:EC2/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B
CryptoCurrency:EC2/BitcoinTool.B!DNS	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B!DNS

GuardDuty Findetyp	ASFF-Ergebnistyp
CryptoCurrency:Lambda/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Lambda-BitcoinTool.B Effects/Resource Consumption/CryptoCurrency:Lambda-BitcoinTool.B
CryptoCurrency:Runtime/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B
CryptoCurrency:Runtime/BitcoinTool.B!DNS	TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B!DNS
DefenseEvasion:EC2/UnusualDNSResolver	TTPs/DefenseEvasion/EC2:Unusual-DNS-Resolver
DefenseEvasion:EC2/UnusualDoHActivity	TTPs/DefenseEvasion/EC2:Unusual-DoH-Activity
DefenseEvasion:EC2/UnusualDoTActivity	TTPs/DefenseEvasion/EC2:Unusual-DoT-Activity
DefenseEvasion:IAMUser/AnomalousBehavior	TTPs/Defense Evasion/IAMUser-AnomalousBehavior
DefenseEvasion:IAMUser/BedrockLoggingDisabled	TTPs/Defense Evasion/DefenseEvasion:IAMUser-BedrockLoggingDisabled
DefenseEvasion:Kubernetes/MaliciousIPCaller	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-MaliciousIPCaller
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-MaliciousIPCaller.Custom
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-SuccessfulAnonymousAccess
DefenseEvasion:Kubernetes/TorIPCaller	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-TorIPCaller

GuardDuty Findetyp	ASFF-Ergebnistyp
DefenseEvasion:Runtime/FilelessExecution	TTPs/Defense Evasion/DefenseEvasion:Runtime-FilelessExecution
DefenseEvasion:Runtime/KernelModuleLoaded	TTPs/Defense Evasion/DefenseEvasion:Runtime-KernelModuleLoaded
DefenseEvasion:Runtime/SensitiveFileModified	TTPs/Defense Evasion/DefenseEvasion:Runtime-SensitiveFileModified
DefenseEvasion:Runtime/ProcessInjection.Proc	TTPs/Defense Evasion/DefenseEvasion:Runtime-ProcessInjection.Proc
DefenseEvasion:Runtime/ProcessInjection.Ptrace	TTPs/Defense Evasion/DefenseEvasion:Runtime-ProcessInjection.Ptrace
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite	TTPs/Defense Evasion/DefenseEvasion:Runtime-ProcessInjection.VirtualMemoryWrite
DefenseEvasion:Runtime/PtraceAntiDebugging	TTPs/DefenseEvasion/DefenseEvasion:Runtime-PtraceAntiDebugging
DefenseEvasion:Runtime/SuspiciousCommand	TTPs/DefenseEvasion/DefenseEvasion:Runtime-SuspiciousCommand
Discovery:IAMUser/AnomalousBehavior	TTPs/Discovery/IAMUser-AnomalousBehavior
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	TTPs/AnomalousBehavior/Discovery:Kubernetes-PermissionChecked
Discovery:Kubernetes/MaliciousIPCaller	TTPs/Discovery/Discovery:Kubernetes-MaliciousIPCaller
Discovery:Kubernetes/MaliciousIPCaller.Custom	TTPs/Discovery/Discovery:Kubernetes-MaliciousIPCaller.Custom
Discovery:Kubernetes/SuccessfulAnonymousAccess	TTPs/Discovery/Discovery:Kubernetes-SuccessfulAnonymousAccess

GuardDuty Findetyp	ASFF-Ergebnistyp
Discovery:Kubernetes/TorIPCaller	TTPs/Discovery/Discovery:Kubernetes-TorIPCaller
Discovery:RDS/MaliciousIPCaller	TTPs/Discovery/RDS-MaliciousIPCaller
Discovery:RDS/TorIPCaller	TTPs/Discovery/RDS-TorIPCaller
Discovery:Runtime/SuspiciousCommand	TTPs/Discovery/Discovery:Runtime-SuspiciousCommand
Discovery:S3/AnomalousBehavior	TTPs/Discovery:S3-AnomalousBehavior
Discovery:S3/BucketEnumeration.Unusual	TTPs/Discovery:S3-BucketEnumeration.Unusual
Discovery:S3/MaliciousIPCaller.Custom	TTPs/Discovery:S3-MaliciousIPCaller.Custom
Discovery:S3/TorIPCaller	TTPs/Discovery:S3-TorIPCaller
Discovery:S3/MaliciousIPCaller	TTPs/Discovery:S3-MaliciousIPCaller
Exfiltration:IAMUser/AnomalousBehavior	TTPs/Exfiltration/IAMUser-AnomalousBehavior
Execution:Kubernetes/ExecInKubeSystemPod	TTPs/Execution/Execution:Kubernetes-ExecInKubeSystemPod
Execution:Kubernetes/AnomalousBehavior.ExecInPod	TTPs/AnomalousBehavior/Execution:Kubernetes-ExecInPod
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	TTPs/AnomalousBehavior/Execution:Kubernetes-WorkloadDeployed
Impact:EC2/MaliciousDomainRequest.Custom	TTPs/Impact/Impact:EC2-MaliciousDomainRequest.Custom
Impact:Kubernetes/MaliciousIPCaller	TTPs/Impact/Impact:Kubernetes-MaliciousIPCaller

GuardDuty Findetyp	ASFF-Ergebnistyp
Impact:Kubernetes/MaliciousIPCaller.Custom	TTPs/Impact/Impact:Kubernetes-MaliciousIPCaller.Custom
Impact:Kubernetes/SuccessfulAnonymousAccess	TTPs/Impact/Impact:Kubernetes-SuccessfulAnonymousAccess
Impact:Kubernetes/TorIPCaller	TTPs/Impact/Impact:Kubernetes-TorIPCaller
Persistence:Kubernetes/ContainerWithSensitiveMount	TTPs/Persistence/Persistence:Kubernetes-ContainerWithSensitiveMount
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	TTPs/AnomalousBehavior/Persistence:Kubernetes-WorkloadDeployed!ContainerWithSensitiveMount
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-WorkloadDeployed!PrivilegedContainer
Persistence:Kubernetes/MaliciousIPCaller	TTPs/Persistence/Persistence:Kubernetes-MaliciousIPCaller
Persistence:Kubernetes/MaliciousIPCaller.Custom	TTPs/Persistence/Persistence:Kubernetes-MaliciousIPCaller.Custom
Persistence:Kubernetes/SuccessfulAnonymousAccess	TTPs/Persistence/Persistence:Kubernetes-SuccessfulAnonymousAccess
Persistence:Kubernetes/TorIPCaller	TTPs/Persistence/Persistence:Kubernetes-TorIPCaller
Execution:EC2/MaliciousFile	TTPs/Execution/Execution:EC2-MaliciousFile
Execution:ECS/MaliciousFile	TTPs/Execution/Execution:ECS-MaliciousFile
Execution:Kubernetes/MaliciousFile	TTPs/Execution/Execution:Kubernetes-MaliciousFile

GuardDuty Findetyp	ASFF-Ergebnistyp
Execution:Container/MaliciousFile	TTPs/Execution/Execution:Container-MaliciousFile
Execution:EC2/SuspiciousFile	TTPs/Execution/Execution:EC2-SuspiciousFile
Execution:ECS/SuspiciousFile	TTPs/Execution/Execution:ECS-SuspiciousFile
Execution:Kubernetes/SuspiciousFile	TTPs/Execution/Execution:Kubernetes-SuspiciousFile
Execution:Container/SuspiciousFile	TTPs/Execution/Execution:Container-SuspiciousFile
Execution:EC2/MaliciousFile!Snapshot	TTPs/Execution/Execution:EC2-MaliciousFile!Snapshot
Execution:EC2/MaliciousFile!AMI	TTPs/Execution/Execution:EC2-MaliciousFile!AMI
Execution:EC2/MaliciousFile!RecoveryPoint	TTPs/Execution/Execution:EC2-MaliciousFile!RecoveryPoint
Execution:S3/MaliciousFile!RecoveryPoint	TTPs/Execution/Execution:S3-MaliciousFile!RecoveryPoint
Execution:Runtime/MaliciousFileExecuted	TTPs/Execution/Execution:Runtime-MaliciousFileExecuted
Execution:Runtime/MaliciousFileExecuted.Custom	TTPs/Execution/Execution:Runtime-MaliciousFileExecuted.Custom
Execution:Runtime/NewBinaryExecuted	TTPs/Execution/Execution:Runtime-NewBinaryExecuted
Execution:Runtime/NewLibraryLoaded	TTPs/Execution/Execution:Runtime-NewLibraryLoaded

GuardDuty Findetyp	ASFF-Ergebnistyp
Execution:Runtime/ReverseShell	TTPs/Execution/Execution:Runtime-ReverseShell
Execution:Runtime/SuspiciousCommand	TTPs/Execution/Execution:Runtime-SuspiciousCommand
Execution:Runtime/SuspiciousShellCreated	TTPs/Execution/Execution:Runtime-SuspiciousShellCreated
Execution:Runtime/SuspiciousTool	TTPs/Execution/Execution:Runtime-SuspiciousTool
Exfiltration:S3/AnomalousBehavior	TTPs/Exfiltration:S3-AnomalousBehavior
Exfiltration:S3/ObjectRead.Unusual	TTPs/Exfiltration:S3-ObjectRead.Unusual
Exfiltration:S3/MaliciousIPCaller	TTPs/Exfiltration:S3-MaliciousIPCaller
Impact:EC2/AbusedDomainRequest.Reputation	TTPs/Impact:EC2-AbusedDomainRequest.Reputation
Impact:EC2/BitcoinDomainRequest.Reputation	TTPs/Impact:EC2-BitcoinDomainRequest.Reputation
Impact:EC2/MaliciousDomainRequest.Reputation	TTPs/Impact:EC2-MaliciousDomainRequest.Reputation
Impact:EC2/PortSweep	TTPs/Impact/Impact:EC2-PortSweep
Impact:EC2/SuspiciousDomainRequest.Reputation	TTPs/Impact:EC2-SuspiciousDomainRequest.Reputation
Impact:EC2/WinRMBruteForce	TTPs/Impact/Impact:EC2-WinRMBruteForce
Impact:IAMUser/AnomalousBehavior	TTPs/Impact/IAMUser-AnomalousBehavior
Impact:Runtime/AbusedDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-AbusedDomainRequest.Reputation

GuardDuty Findetyp	ASFF-Ergebnistyp
Impact:Runtime/BitcoinDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-BitcoinDomainRequest.Reputation
Impact:Runtime/CryptoMinerExecuted	TTPs/Impact/Impact:Runtime-CryptoMinerExecuted
Impact:Runtime/MaliciousDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation
Impact:Runtime/SuspiciousDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-SuspiciousDomainRequest.Reputatio
Impact:S3/AnomalousBehavior.Delete	TTPs/Impact:S3-AnomalousBehavior.Delete
Impact:S3/AnomalousBehavior.Permission	TTPs/Impact:S3-AnomalousBehavior.Permission
Impact:S3/AnomalousBehavior.Write	TTPs/Impact:S3-AnomalousBehavior.Write
Impact:S3/ObjectDelete.Unusual	TTPs/Impact:S3-ObjectDelete.Unusual
Impact:S3/PermissionsModification.Unusual	TTPs/Impact:S3-PermissionsModification.Unusual
Impact:S3/MaliciousIPCaller	TTPs/Impact:S3-MaliciousIPCaller
InitialAccess:IAMUser/AnomalousBehavior	TTPs/Initial Access/IAMUser-AnomalousBehavior
Object:S3/MaliciousFile	TTPs/Object/Object:S3-MaliciousFile
PenTest:IAMUser/KaliLinux	TTPs/PenTest:IAMUser/KaliLinux
PenTest:IAMUser/ParrotLinux	TTPs/PenTest:IAMUser/ParrotLinux
PenTest:IAMUser/PentooLinux	TTPs/PenTest:IAMUser/PentooLinux
PenTest:S3/KaliLinux	TTPs/PenTest:S3-KaliLinux

GuardDuty Findetyp	ASFF-Ergebnistyp
PenTest:S3/ParrotLinux	TTPs/PenTest:S3-ParrotLinux
PenTest:S3/PentooLinux	TTPs/PenTest:S3-PentooLinux
Persistence:IAMUser/AnomalousBehavior	TTPs/Persistence/IAMUser-AnomalousBehavior
Persistence:IAMUser/NetworkPermissions	TTPs/Persistence/Persistence:IAMUser-NetworkPermissions
Persistence:IAMUser/ResourcePermissions	TTPs/Persistence/Persistence:IAMUser-ResourcePermissions
Persistence:IAMUser/UserPermissions	TTPs/Persistence/Persistence:IAMUser-UserPermissions
Persistence:Runtime/SuspiciousCommand	TTPs/Persistence/Persistence:Runtime-SuspiciousCommand
Persistence:Runtime/SensitiveFileModified	TTPs/Persistence/Persistence:Runtime-SensitiveFileModified
Policy:IAMUser/RootCredentialUsage	TTPs/Policy:IAMUser-RootCredentialUsage
Policy:IAMUser/ShortTermRootCredentialUsage	TTPs/Policy:IAMUser-ShortTermRootCredentialUsage
Policy:Kubernetes/AdminAccessToDefaultServiceAccount	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-AdminAccessToDefaultServiceAccount
Policy:Kubernetes/AnonymousAccessGranted	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-AnonymousAccessGranted
Policy:Kubernetes/ExposedDashboard	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-ExposedDashboard

GuardDuty Findetyp	ASFF-Ergebnistyp
Policy:Kubernetes/KubeflowDashboardExposed	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-KubeflowDashboardExposed
Policy:S3/AccountBlockPublicAccessDisabled	TTPs/Policy:S3-AccountBlockPublicAccessDisabled
Policy:S3/BucketAnonymousAccessGranted	TTPs/Policy:S3-BucketAnonymousAccessGranted
Policy:S3/BucketBlockPublicAccessDisabled	Effects/Data Exposure/Policy:S3-BucketBlockPublicAccessDisabled
Policy:S3/BucketPublicAccessGranted	TTPs/Policy:S3-BucketPublicAccessGranted
PrivilegeEscalation:IAMUser/AnomalousBehavior	TTPs/Privilege Escalation/IAMUser-AnomalousBehavior
PrivilegeEscalation:IAMUser/AdministrativePermissions	TTPs/Privilege Escalation/PrivilegeEscalation:IAMUser-AdministrativePermissions
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-RoleBindingCreated
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-RoleCreated
PrivilegeEscalation:Kubernetes/PrivilegedContainer	TTPs/PrivilegeEscalation/PrivilegeEscalation:Kubernetes-PrivilegedContainer
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-ContainerMountsHostDirectory
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-CGroupsReleaseAgentModified
PrivilegeEscalation:Runtime/DockerSocketAccessed	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-DockerSocketAccessed

GuardDuty Findetyp	ASFF-Ergebnistyp
PrivilegeEscalation:Runtime/ElevationToRoot	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-ElevationToRoot
PrivilegeEscalation:Runtime/RuncContainerEscape	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-RuncContainerEscape
PrivilegeEscalation:Runtime/SuspiciousCommand	Software and Configuration Checks/PrivilegeEscalation:Runtime-SuspiciousCommand
PrivilegeEscalation:Runtime/SensitiveFileModified	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-SensitiveFileModified
PrivilegeEscalation:Runtime/UserfaultfdUsage	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-UserfaultfdUsage
Recon:EC2/PortProbeEMRUnprotectedPort	TTPs/Discovery/Recon:EC2-PortProbeEMRUnprotectedPort
Recon:EC2/PortProbeUnprotectedPort	TTPs/Discovery/Recon:EC2-PortProbeUnprotectedPort
Recon:EC2/Portscan	TTPs/Discovery/Recon:EC2-Portscan
Recon:IAMUser/MaliciousIPCaller	TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller
Recon:IAMUser/MaliciousIPCaller.Custom	TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller.Custom
Recon:IAMUser/NetworkPermissions	TTPs/Discovery/Recon:IAMUser-NetworkPermissions
Recon:IAMUser/ResourcePermissions	TTPs/Discovery/Recon:IAMUser-ResourcePermissions
Recon:IAMUser/TorIPCaller	TTPs/Discovery/Recon:IAMUser-TorIPCaller

GuardDuty Findetyp	ASFF-Ergebnistyp
Recon:IAMUser/UserPermissions	TTPs/Discovery/Recon:IAMUser-UserPermissions
ResourceConsumption:IAMUser/ComputeResources	Unusual Behaviors/User/ResourceConsumption:IAMUser-ComputeResources
Stealth:IAMUser/CloudTrailLoggingDisabled	TTPs/Defense Evasion/Stealth:IAMUser-CloudTrailLoggingDisabled
Stealth:IAMUser/LoggingConfigurationModified	TTPs/Defense Evasion/Stealth:IAMUser-LoggingConfigurationModified
Stealth:IAMUser/PasswordPolicyChange	TTPs/Defense Evasion/Stealth:IAMUser-PasswordPolicyChange
Stealth:S3/ServerAccessLoggingDisabled	TTPs/Defense Evasion/Stealth:S3-ServerAccessLoggingDisabled
Trojan:EC2/BlackholeTraffic	TTPs/Command and Control/Trojan:EC2-BlackholeTraffic
Trojan:EC2/BlackholeTraffic!DNS	TTPs/Command and Control/Trojan:EC2-BlackholeTraffic!DNS
Trojan:EC2/DGADomainRequest.B	TTPs/Command and Control/Trojan:EC2-DGADomainRequest.B
Trojan:EC2/DGADomainRequest.C!DNS	TTPs/Command and Control/Trojan:EC2-DGADomainRequest.C!DNS
Trojan:EC2/DNSDataExfiltration	TTPs/Command and Control/Trojan:EC2-DNSDataExfiltration
Trojan:EC2/DriveBySourceTraffic!DNS	TTPs/Initial Access/Trojan:EC2-DriveBySourceTraffic!DNS
Trojan:EC2/DropPoint	Effects/Data Exfiltration/Trojan:EC2-DropPoint

GuardDuty Findetyp	ASFF-Ergebnistyp
Trojan:EC2/DropPoint!DNS	Effects/Data Exfiltration/Trojan:EC2-DropPoint!DNS
Trojan:EC2/PhishingDomainRequest!DNS	TTPs/Command and Control/Trojan:EC2-PhishingDomainRequest!DNS
Trojan:Lambda/BlackholeTraffic	TTPs/Command and Control/Trojan:Lambda-BlackholeTraffic
Trojan:Lambda/DropPoint	Effects/Data Exfiltration/Trojan:Lambda-DropPoint
Trojan:Runtime/BlackholeTraffic	TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic
Trojan:Runtime/BlackholeTraffic!DNS	TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic!DNS
Trojan:Runtime/DGADomainRequest.C!DNS	TTPs/Command and Control/Trojan:Runtime-DGADomainRequest.C!DNS
Trojan:Runtime/DriveBySourceTraffic!DNS	TTPs/Initial Access/Trojan:Runtime-DriveBySourceTraffic!DNS
Trojan:Runtime/DropPoint	Effects/Data Exfiltration/Trojan:Runtime-DropPoint
Trojan:Runtime/DropPoint!DNS	Effects/Data Exfiltration/Trojan:Runtime-DropPoint!DNS
Trojan:Runtime/PhishingDomainRequest!DNS	TTPs/Command and Control/Trojan:Runtime-PhishingDomainRequest!DNS
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	TTPs/Command and Control/UnauthorizedAccess:EC2-MaliciousIPCaller.Custom
UnauthorizedAccess:EC2/MetadataDNSRebind	TTPs/UnauthorizedAccess:EC2-MetadataDNSRebind

GuardDuty Findetyp	ASFF-Ergebnistyp
UnauthorizedAccess:EC2/RDPBruteForce	TTPs/Initial Access/UnauthorizedAccess:EC2-RDPBruteForce
UnauthorizedAccess:EC2/SSHBruteForce	TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce
UnauthorizedAccess:EC2/TorClient	Effects/Resource Consumption/UnauthorizedAccess:EC2-TorClient
UnauthorizedAccess:EC2/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:EC2-TorRelay
UnauthorizedAccess:IAMUser/ConsoleLogin	Unusual Behaviors/User/UnauthorizedAccess:IAMUser-ConsoleLogin
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	TTPs/UnauthorizedAccess:IAMUser-ConsoleLoginSuccess.B
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.InsideAWS
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.OutsideAWS
UnauthorizedAccess:IAMUser/MaliciousIPCaller	TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller.Custom
UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-ResourceCredentialExfiltration.InsideAWS

GuardDuty Findetyp	ASFF-Ergebnistyp
UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-ResourceCredentialExfiltration.OutsideAWS
UnauthorizedAccess:IAMUser/TorIPCaller	TTPs/Command and Control/UnauthorizedAccess:IAMUser-TorIPCaller
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	TTPs/Command and Control/UnauthorizedAccess:Lambda-MaliciousIPCaller.Custom
UnauthorizedAccess:Lambda/TorClient	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorClient
UnauthorizedAccess:Lambda/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorRelay
UnauthorizedAccess:Runtime/MetadataDNSRebind	TTPs/UnauthorizedAccess:Runtime-MetadataDNSRebind
UnauthorizedAccess:Runtime/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorRelay
UnauthorizedAccess:Runtime/TorClient	Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorClient
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	TTPs/UnauthorizedAccess:S3-MaliciousIPCaller.Custom
UnauthorizedAccess:S3/TorIPCaller	TTPs/UnauthorizedAccess:S3-TorIPCaller

Typischer Befund von GuardDuty

GuardDuty sendet Ergebnisse mithilfe des Security Finding Formats (ASFF) an AWS Security Hub CSPM.

Hier ist ein Beispiel für ein typisches Ergebnis von. GuardDuty

```
  {
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64/finding/46ba0ac2845071e23ccdeb2ae03bfdea",
  "ProductArn": "arn:aws:securityhub:us-east-1:product/aws/guardduty",
  "GeneratorId": "arn:aws:guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64",
  "AwsAccountId": "193043430472",
  "Types": [
    "TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce"
  ],
  "FirstObservedAt": "2020-08-22T09:15:57Z",
  "LastObservedAt": "2020-09-30T11:56:49Z",
  "CreatedAt": "2020-08-22T09:34:34.146Z",
  "UpdatedAt": "2020-09-30T12:14:00.206Z",
  "Severity": {
    "Product": 2,
    "Label": "MEDIUM",
    "Normalized": 40
  },
  "Title": "199.241.229.197 is performing SSH brute force attacks against
 i-0c10c2c7863d1a356.",
  "Description": "199.241.229.197 is performing SSH brute force attacks against
 i-0c10c2c7863d1a356. Brute force attacks are used to gain unauthorized access to your
 instance by guessing the SSH password.",
  "SourceUrl": "https://us-east-1.console.aws.amazon.com/guardduty/home?region=us-
east-1#/findings?macros=current&fId=46ba0ac2845071e23ccdeb2ae03bfdea",
  "ProductFields": {
    "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/portName":
 "Unknown",
    "aws/guardduty/service/archived": "false",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asnOrg": "CENTURYLINK-US-LEGACY-QWEST",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lat": "42.5122",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/ipAddressV4":
 "199.241.229.197",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lon": "-90.7384",
    "aws/guardduty/service/action/networkConnectionAction/blocked": "false",
    "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/port":
 "46717",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/country/
countryName": "United States",
```

```
    "aws/guardduty/service/serviceName": "guardduty",
    "aws/guardduty/service/evidence": "",
    "aws/guardduty/service/action/networkConnectionAction/localIpDetails/ipAddressV4":
 "172.31.43.6",
    "aws/guardduty/service/detectorId": "d4b040365221be2b54a6264dc9a4bc64",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
org": "CenturyLink",
    "aws/guardduty/service/action/networkConnectionAction/connectionDirection":
 "INBOUND",
    "aws/guardduty/service/eventFirstSeen": "2020-08-22T09:15:57Z",
    "aws/guardduty/service/eventLastSeen": "2020-09-30T11:56:49Z",
    "aws/guardduty/service/action/networkConnectionAction/localPortDetails/portName":
 "SSH",
    "aws/guardduty/service/action/actionType": "NETWORK_CONNECTION",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/city/
cityName": "Dubuque",
    "aws/guardduty/service/additionalInfo": "",
    "aws/guardduty/service/resourceRole": "TARGET",
    "aws/guardduty/service/action/networkConnectionAction/localPortDetails/port": "22",
    "aws/guardduty/service/action/networkConnectionAction/protocol": "TCP",
    "aws/guardduty/service/count": "74",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asn": "209",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
isp": "CenturyLink",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/guardduty/
arn:aws:guardduty:us-east-1:193043430472:detector/d4b040365221be2b54a6264dc9a4bc64/
finding/46ba0ac2845071e23ccdeb2ae03bfdea",
    "aws/securityhub/ProductName": "GuardDuty",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "arn:aws:ec2:us-east-1:193043430472:instance/i-0c10c2c7863d1a356",
      "Partition": "aws",
      "Region": "us-east-1",
      "Tags": {
        "Name": "kubectl"
      },
      "Details": {
        "AwsEc2Instance": {
          "Type": "t2.micro",
          "ImageId": "ami-02354e95b39ca8dec",
```

```
          "IpV4Addresses": [
            "18.234.130.16",
            "172.31.43.6"
          ],
          "VpcId": "vpc-a0c2d7c7",
          "SubnetId": "subnet-4975b475",
          "LaunchedAt": "2020-08-03T23:21:57Z"
        }
      }
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE"
}
```

Aktivieren und Konfigurieren der Integration

Um die Integration mit verwenden zu können AWS Security Hub CSPM, müssen Sie Security Hub CSPM aktivieren. Informationen zur Aktivierung von Security Hub CSPM finden Sie unter Security Hub einrichten im AWS Security Hub Benutzerhandbuch.

Wenn Sie GuardDuty sowohl als auch Security Hub CSPM aktivieren, wird die Integration automatisch aktiviert. GuardDutybeginnt sofort, Ergebnisse an Security Hub CSPM zu senden.

Verwendung von GuardDuty Steuerelementen in Security Hub CSPM

AWS Security Hub CSPM verwendet Sicherheitskontrollen, um Ihre AWS Ressourcen zu bewerten und zu überprüfen, ob Sie die Sicherheitsstandards und bewährten Verfahren der Branche einhalten. Sie können die Kontrollen verwenden, die sich auf GuardDuty Ressourcen und ausgewählte Schutzpläne beziehen. Weitere Informationen finden Sie unter Amazon GuardDuty Controls im AWS Security Hub Benutzerhandbuch.

Eine Liste aller Kontrollen für AWS Dienste und Ressourcen finden Sie unter Security Hub CSPM-Steuerungsreferenz im AWS Security Hub Benutzerhandbuch.

Einstellung der Veröffentlichung der Ergebnisse im Security Hub CSPM

Um anzugeben, dass keine Erkenntnisse mehr an Security Hub CSPM gesendet werden, können Sie entweder die Konsole von Security Hub CSPM oder die API verwenden.

Weitere Informationen finden Sie unter Deaktivieren und Aktivieren des Ergebnisflusses aus einer Integration (Konsole) oder Deaktivieren des Ergebnisflusses aus einer Integration (Security Hub Hub-API, AWS CLI) im AWS Security Hub Benutzerhandbuch.

Integration mit Amazon Detective

Amazon Detective hilft Ihnen dabei, Sicherheitsereignisse in einem oder mehreren AWS Konten schnell zu analysieren und zu untersuchen, indem es Datenvisualisierungen generiert, die das Verhalten und die Interaktion Ihrer Ressourcen im Laufe der Zeit darstellen. Detective erstellt Visualisierungen von Ergebnissen. GuardDuty

Detective nimmt Erkenntnisdetails für alle Erkenntnistypen auf und bietet Zugriff auf die Entitätsprofile, um verschiedene Entitäten zu untersuchen, die an der Erkenntnis beteiligt sind. Eine Entität kann eine AWS-Konto, eine AWS Ressource innerhalb eines Kontos oder eine externe IP-Adresse sein, die mit Ihren Ressourcen interagiert hat. Die GuardDuty Konsole unterstützt je nach Findetyp das Pivotieren von den folgenden Entitäten zu Amazon Detective: AWS-Konto, IAM-Rolle, Benutzer- oder Rollensitzung, Benutzeragent, Verbundbenutzer, Amazon EC2 EC2-Instance oder IP-Adresse.

Inhalt

- Aktivierung der Integration
- Von einem GuardDuty Befund zu Amazon Detective wechseln
- Verwendung der Integration in einer Umgebung mit GuardDuty mehreren Konten

Aktivierung der Integration

Um Amazon Detective mit verwenden zu können, müssen GuardDuty Sie zuerst Amazon Detective aktivieren. Informationen zur Aktivierung von Detective finden Sie unter Erste Schritte mit Amazon Detective im Amazon Detective-Benutzerhandbuch.

Wenn Sie GuardDuty sowohl als auch Detective aktivieren, wird die Integration automatisch aktiviert. Nach der Aktivierung nimmt Detective Ihre GuardDuty Ergebnisdaten sofort auf.

> **Note**
>
> GuardDuty sendet Ergebnisse basierend auf der Häufigkeit des Exports der GuardDuty Ergebnisse an Detective. Standardmäßig beträgt die Exporthäufigkeit für Aktualisierungen

vorhandener Erkenntnisse 6 Stunden. Um sicherzustellen, dass Detective die neuesten Aktualisierungen Ihrer Ergebnisse erhält, wird empfohlen, die Exporthäufigkeit in jeder Region, in der Sie Detective verwenden, auf 15 Minuten zu ändern GuardDuty. Weitere Informationen finden Sie unter Schritt 5 — Häufigkeit für den Export aktualisierter aktiver Ergebnisse festlegen.

Von einem GuardDuty Befund zu Amazon Detective wechseln

1. Loggen Sie sich in die https://console.aws.amazon.com/guardduty/Konsole ein.
2. Wählen Sie eine einzelne Erkenntnis aus Ihrer Erkenntnistabelle aus.
3. Wählen Sie im Bereich mit den Erkenntnisdetails die Option Mit Detective untersuchen.
4. Wählen Sie einen Aspekt der Erkenntnis aus, den Sie mit Amazon Detective untersuchen möchten. Dadurch wird die Detective-Konsole für diese Erkenntnis oder diese Entität geöffnet.

Wenn sich der Wechsel nicht wie erwartet verhält, finden Sie weitere Informationen unter Fehlerbehebung beim Wechsel im Amazon-Detective-Benutzerhandbuch.

> **Note**
>
> Wenn Sie ein GuardDuty Ergebnis in der Detective-Konsole archivieren, wird dieses Ergebnis auch in der GuardDuty Konsole archiviert.

Verwendung der Integration in einer Umgebung mit GuardDuty mehreren Konten

Wenn Sie eine Umgebung mit mehreren Konten in verwalten GuardDuty, müssen Sie Ihre Mitgliedskonten zu Amazon Detective hinzufügen, um Detective-Datenvisualisierungen für Ergebnisse und Entitäten in diesen Konten anzuzeigen.

Es wird empfohlen, dasselbe GuardDuty Administratorkonto wie das Administratorkonto für Detective zu verwenden. Weitere Informationen zum Hinzufügen von Mitgliedskonten in Detective finden Sie unter Konten verwalten im Amazon Detective User Guide.

> **Note**
>
> Detective ist ein regionaler Service, d. h. Sie müssen Detective aktivieren und Ihre Mitgliedskonten in jeder Region hinzufügen, in der Sie die Integration verwenden möchten.

Aussetzen oder Deaktivieren GuardDuty

Sie können die GuardDuty Konsole verwenden, um den GuardDuty Service auszusetzen oder zu deaktivieren. Die Nutzung wird Ihnen nicht in Rechnung gestellt GuardDuty , wenn der Dienst gesperrt ist.

- Alle Mitgliedskonten müssen getrennt oder gelöscht werden, bevor Sie sie sperren oder deaktivieren GuardDuty können.
- Wenn Sie die GuardDuty Sperre sperren, wird die Sicherheit Ihrer AWS Umgebung nicht mehr überwacht und es werden keine neuen Erkenntnisse mehr generiert. Ihre vorhandenen Ergebnisse bleiben erhalten und sind von der GuardDuty Sperrung nicht betroffen. Sie können wählen, ob Sie es GuardDuty später wieder aktivieren möchten.
- Wenn Sie es GuardDuty in einem Konto deaktivieren, wird es nur für das aktuell ausgewählte AWS-Region Konto deaktiviert. Wenn Sie es vollständig deaktivieren möchten GuardDuty, müssen Sie es in jeder Region deaktivieren, in der es aktiviert ist.
- Wenn Sie es deaktivieren GuardDuty, gehen Ihre vorhandenen Ergebnisse und die GuardDuty Konfiguration verloren und können nicht wiederhergestellt werden. Wenn Sie Ihre vorhandenen Ergebnisse speichern möchten, müssen Sie sie exportieren, bevor Sie die Deaktivierung bestätigen GuardDuty. Weitere Informationen zum Exportieren von Erkenntnissen finden Sie unter Generierte Ergebnisse nach Amazon S3 exportieren.
- Wenn Sie Malware Protection for S3 für einen oder mehrere geschützte Buckets in Ihrem Konto aktiviert haben, wirkt sich das Sperren oder Deaktivieren GuardDuty nicht auf den Status eines geschützten Buckets unter Malware Protection for S3 aus. Auch nach der Sperrung oder Deaktivierung fallen für Ihr Konto weiterhin die Nutzungskosten an GuardDuty, die mit der Funktion „Malware-Schutz für S3“ verbunden sind. Informationen zur Deaktivierung von Malware Protection for S3 finden Sie unter. Malware-Schutz für S3 für einen geschützten Bucket deaktivieren

So sperren oder deaktivieren Sie GuardDuty

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie im GuardDutyAbschnitt Sperren die Option Sperren GuardDuty oder Deaktivieren aus GuardDuty und bestätigen Sie dann Ihre Aktion.

Um die Aktivierung nach GuardDuty dem Aussetzen erneut zu aktivieren

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie Re-enable GuardDuty.

Amazon GuardDuty SNS SNS-Ankündigungen abonnieren

Dieser Abschnitt enthält Informationen zum Abonnieren von Amazon SNS (Simple Notification Service) für GuardDuty Ankündigungen, Benachrichtigungen über neu veröffentlichte Befundtypen, Aktualisierungen der vorhandenen Befundtypen und andere Funktionsänderungen zu erhalten. Benachrichtigungen sind in allen Formaten verfügbar, die Amazon SNS unterstützt.

Der GuardDuty SNS sendet Ankündigungen über Aktualisierungen des GuardDuty Dienstes AWS an jedes abonnierte Konto. Informationen, um Benachrichtigungen über Erkenntnisse in Ihrem Konto zu erhalten, finden Sie unter Bearbeitung von GuardDuty Ergebnissen mit Amazon EventBridge.

> **Note**
>
> Ihr IAM-Benutzer muss `sns::subscribe`-Berechtigungen haben, ein SNS zu abonnieren.

Sie können eine Amazon SQS-Warteschlange für dieses Benachrichtigungsthema abonnieren, aber Sie müssen einen Themen-ARN verwenden, der sich in derselben Region befindet. Weitere Informationen finden Sie unter Tutorial: Abonnieren einer Amazon-SQS-Warteschlange zu einem Amazon-SNS-Thema im Entwicklerhandbuch für Amazon Simple Queue Service.

Sie können auch eine AWS Lambda Funktion verwenden, um Ereignisse auszulösen, wenn Benachrichtigungen eingehen. Weitere Informationen finden Sie unter Aufrufen von Lambda-Funktionen mit Amazon-SNS-Benachrichtigungen im Enwicklerhandbuch für Amazon Simple Queue Service.

Die Amazon SNS-Thema-ARNs für jede Region sind unten aufgeführt.

AWS-Region	ARN des Amazon-SNS-Themas
USA Ost (Nord-Virginia) – `us-east-1`	`arn:aws:sns:us-east-1:242987662583:GuardDutyAnnouncements`
USA Ost (Ohio) - `us-east-2`	`arn:aws:sns:us-east-2:118283430703:G`

AWS-Region	ARN des Amazon-SNS-Themas
	uardDutyAnnouncements
USA West (Nordkalifornien) - us-west-1	arn:aws:sns:us-west-1:144182107116:GuardDutyAnnouncements
USA West (Oregon) – us-west-2	arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements
Kanada (Zentral) - ca-central-1	arn:aws:sns:ca-central-1:107430051933:GuardDutyAnnouncements
Kanada West (Calgary) - ca-west-1	arn:aws:sns:ca-west-1:440427180217:GuardDutyAnnouncements
Europa (Stockholm) - eu-north-1	arn:aws:sns:eu-north-1:973841112453:GuardDutyAnnouncements
Europa (Irland) - eu-west-1	arn:aws:sns:eu-west-1:965013871422:GuardDutyAnnouncements

AWS-Region	ARN des Amazon-SNS-Themas
Europa (London) - `eu-west-2`	`arn:aws:sns:eu-west-2:506403581195:GuardDutyAnnouncements`
Europa (Paris) - `eu-west-3`	`arn:aws:sns:eu-west-3:436163563069:GuardDutyAnnouncements`
Europa (Frankfurt) - `eu-central-1`	`arn:aws:sns:eu-central-1:378365507264:GuardDutyAnnouncements`
Europa (Zürich) - `eu-central-2`	`arn:aws:sns:eu-central-2:383009515534:GuardDutyAnnouncements`
Asien-Pazifik (Hongkong) - `ap-east-1`	`arn:aws:sns:ap-east-1:646602203151:GuardDutyAnnouncements`
Asien-Pazifik (Tokio) – `ap-northeast-1`	`arn:aws:sns:ap-northeast-1:741172661024:GuardDutyAnnouncements`
Asien-Pazifik (Seoul) - `ap-northeast-2`	`arn:aws:sns:ap-northeast-2:464168911255:GuardDutyAnnouncements`

AWS-Region	ARN des Amazon-SNS-Themas
Asien-Pazifik (Singapur) - `ap-southeast-1`	`arn:aws:sns:ap-southeast-1:476419727788:GuardDutyAnnouncements`
Asien-Pazifik (Sydney) - `ap-southeast-2`	`arn:aws:sns:ap-southeast-2:457615622431:GuardDutyAnnouncements`
Asien-Pazifik (Mumbai) - `ap-south-1`	`arn:aws:sns:ap-south-1:926826061926:GuardDutyAnnouncements`
Südamerika (São Paulo) - `sa-east-1`	`arn:aws:sns:sa-east-1:955633302743:GuardDutyAnnouncements`
AWS GovCloud (US-West) - `us-gov-west-1`	`arn:aws-us-gov:sns:us-gov-west-1:430639793359:GuardDutyAnnouncements`
China (Peking) - `cn-north-1`	`arn:aws-cn:sns:cn-north-1:002991280229:GuardDutyAnnouncements`
China (Ningxia) - `cn-northwest-1`	`arn:aws-cn:sns:cn-northwest-1:003033775354:GuardDutyAnnouncements`

AWS-Region	ARN des Amazon-SNS-Themas
Naher Osten (Bahrain) - me-south-1	arn:aws:sns:me-south-1:552740612889:GuardDutyAnnouncements
Naher Osten (VAE) - me-central-1	arn:aws:sns:me-central-1:030935290150:GuardDutyAnnouncements
Europa (Mailand) - eu-south-1	arn:aws:sns:eu-south-1:188461706213:GuardDutyAnnouncements
Europa (Spanien) - eu-south-2	arn:aws:sns:eu-south-2:445632894446:GuardDutyAnnouncements
AWS GovCloud (US-East) - us-gov-east-1	arn:aws:sns:us-gov-east-1:143972945659:GuardDutyAnnouncements
Asien Pazifik (Osaka) – ap-northeast-3	arn:aws:sns:ap-northeast-3:129086577509:GuardDutyAnnouncements
Asien-Pazifik (Jakarta) - ap-southeast-3	arn:aws:sns:ap-southeast-3:225965583551:GuardDutyAnnouncements

AWS-Region	ARN des Amazon-SNS-Themas
Asien-Pazifik (Hyderabad) - `ap-south-2`	`arn:aws:sns:ap-south-2:595653072700:GuardDutyAnnouncements`
Asien-Pazifik (Melbourne) - `ap-southeast-4`	`arn:aws:sns:ap-southeast-4:529900636122:GuardDutyAnnouncements`
Asien-Pazifik (Malaysia) - `ap-southeast-5`	`arn:aws:sns:ap-southeast-5:343218181797:GuardDutyAnnouncements`
Israel (Tel Aviv) - `il-central-1`	`arn:aws:sns:il-central-1:847886274986:GuardDutyAnnouncements`
Asien-Pazifik (Thailand) - `ap-southeast-7`	`arn:aws:sns:ap-southeast-7:863518448376:GuardDutyAnnouncements`
Mexiko (Zentral) - `mx-central-1`	`arn:aws:sns:mx-central-1:060795916546:GuardDutyAnnouncements`
Asien-Pazifik (Taipeh) - `ap-east-2`	`arn:aws:sns:ap-east-2:604225987917:GuardDutyAnnouncements`

Um die GuardDuty Update-Benachrichtigungs-E-Mail im zu abonnieren AWS-Managementkonsole

1. Öffnen Sie die Amazon-SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Wählen Sie in der Regionsliste die gleiche Region aus, wie der Thema-ARN, den Sie abonnieren möchten. In diesem Beispiel wird die Region `us-west-2` verwendet.
3. Wählen Sie im linken Navigationsbereich Subscriptions (Abonnements) und danach Create subscription (Abonnement erstellen) aus.
4. Fügen Sie im Dialogfeld Create Subscription (Abonnement erstellen) unter Topic ARN (Themen-ARN) den Themen-ARN: `arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements` ein.
5. Wählen Sie unter Protocol (Protokoll) die Option Email (E-Mail) aus. Geben Sie unter Endpoint (Endpunkt) eine E-Mail-Adresse ein, um die Benachrichtigung zu empfangen.
6. Wählen Sie Create subscription (Abonnement erstellen) aus.
7. Öffnen Sie in Ihrer E-Mail-Anwendung die Nachricht unter AWS Benachrichtigungen und klicken Sie auf den Link, um Ihr Abonnement zu bestätigen.

   Ihr Webbrowser zeigt eine Bestätigungsantwort vom Amazon SNS an.

Um die GuardDuty Update-Benachrichtigungs-E-Mail mit dem zu abonnieren AWS CLI

1. Führen Sie den folgenden Befehl mit der AWS CLI aus:

```
 aws  sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements --protocol email --notification-
endpoint your_email@your_domain.com
```

2. Öffnen Sie in Ihrer E-Mail-Anwendung die Nachricht unter AWS Benachrichtigungen und klicken Sie auf den Link, um Ihr Abonnement zu bestätigen.

   Ihr Webbrowser zeigt eine Bestätigungsantwort vom Amazon SNS an.

Amazon-SNS-Nachrichtenformat

Ein Beispiel GuardDuty für eine allgemeine Benachrichtigung:

```
{
    "Type" : "Notification",
```

```
    "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message" : "{\"version\":\"1\",\"type\":\"GENERAL\",\"message\":[{\"title\":
\"Updated AmazonGuardDutyFullAccess_v2 policy\",\"body\":\"Added permission that
 allows you to pass an IAM role to GuardDuty when you enable Malware Protection for
 S3.\",\"links\":[\"https://docs.aws.amazon.com//guardduty/latest/ug/security-iam-
awsmanpol.html#security-iam-awsmanpol-AmazonGuardDutyFullAccess-v2\"]}]}",
    "Timestamp" : "2018-03-09T00:25:43.483Z",
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
    "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```


Die geparste Benachrichtigung (mit entfernten Escape-Zeichen) ist nachfolgend gezeigt:


```
{
        "version": "1",
        "type": "GENERAL",
        "message": [
            {
                "title": "Updated AmazonGuardDutyFullAccess policy",
                "body": "Added permission that allows you to pass an IAM role to
 GuardDuty when you enable Malware Protection for S3.",
                "links": [
                    "https://docs.aws.amazon.com//guardduty/latest/ug/security-iam-
awsmanpol.html#security-iam-awsmanpol-AmazonGuardDutyFullAccess-v2"
                ]
             }
        ]
}
```


Im Folgenden finden Sie ein Beispiel für eine GuardDuty Aktualisierungsbenachrichtigung über neue Ergebnisse:

```
{
    "Type" : "Notification",
    "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message" : "{\"version\":\"1\",\"type\":\"NEW_FINDINGS\",\"findingDetails
\":[{\"link\":\"https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html\",\"findingType\":\"UnauthorizedAccess:EC2/TorClient\",
\"findingDescription\":\"This finding informs you that an EC2 instance in your AWS
 environment is making connections to a Tor Guard or an Authority node. Tor is software
 for enabling anonymous communication. Tor Guards and Authority nodes act as initial
 gateways into a Tor network. This traffic can indicate that this EC2 instance is
 acting as a client on a Tor network. A common use for a Tor client is to circumvent
 network monitoring and filter for access to unauthorized or illicit content. Tor
 clients can also generate nefarious Internet traffic, including attacking SSH servers.
 This activity can indicate that your EC2 instance is compromised.\"}]}",
    "Timestamp" : "2018-03-09T00:25:43.483Z",
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
    "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```


Die geparste Benachrichtigung (mit entfernten Escape-Zeichen) ist nachfolgend gezeigt:


```
{
    "version": "1",
    "type": "NEW_FINDINGS",
    "findingDetails": [{
        "link": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html",
        "findingType": "UnauthorizedAccess:EC2/TorClient",
        "findingDescription": "This finding informs you that an EC2 instance in your
 AWS environment is making connections to a Tor Guard or an Authority node. Tor is
 software for enabling anonymous communication. Tor Guards and Authority nodes act as
 initial gateways into a Tor network. This traffic can indicate that this EC2 instance
```

```
 is acting as a client on a Tor network. A common use for a Tor client is to circumvent
 network monitoring and filter for access to unauthorized or illicit content. Tor
 clients can also generate nefarious Internet traffic, including attacking SSH servers.
 This activity can indicate that your EC2 instance is compromised."
    }]
}
```

Im Folgenden finden Sie ein Beispiel für eine GuardDuty Update-Benachrichtigung über GuardDuty Funktionsupdates:

```
{
    "Type" : "Notification",
    "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message" : "{\"version\":\"1\",\"type\":\"NEW_FEATURES\",\"featureDetails
\":[{\"featureDescription\":\"Customers with high-volumes of global CloudTrail
 events should see a net positive impact on their GuardDuty costs.\",\"featureLink
\":\"https://docs.aws.amazon.com//guardduty/latest/ug/guardduty_data-
sources.html#guardduty_controlplane\"}]}",
    "Timestamp" : "2018-03-09T00:25:43.483Z",
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
    "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

Die geparste Benachrichtigung (mit entfernten Escape-Zeichen) ist nachfolgend gezeigt:

```
{
    "version": "1",
    "type": "NEW_FEATURES",
    "featureDetails": [{
        "featureDescription": "Customers with high-volumes of global CloudTrail events
 should see a net positive impact on their GuardDuty costs.",
```

```
        "featureLink": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_data-sources.html#guardduty_controlplane"
    }]
}
```

Im Folgenden finden Sie ein Beispiel für eine GuardDuty Update-Benachrichtigung über aktualisierte Ergebnisse:

```
{
    "Type": "Notification",
    "MessageId": "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn": "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message": "{\"version\":\"1\",\"type\":\"UPDATED_FINDINGS\",
\"findingDetails\":[{\"link\":\"https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html\",\"findingType\":\"UnauthorizedAccess:EC2/TorClient\",
\"description\":\"Increased severity value from 5 to 8.\"}]}",
    "Timestamp": "2018-03-09T00:25:43.483Z",
    "SignatureVersion": "1",
    "Signature": "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

Die geparste Benachrichtigung (mit entfernten Escape-Zeichen) ist nachfolgend gezeigt:

```
{
    "version": "1",
    "type": "UPDATED_FINDINGS",
    "findingDetails": [{
        "link": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html",
        "findingType": "UnauthorizedAccess:EC2/TorClient",
        "description": "Increased severity value from 5 to 8."
    }]
```

```
}
```

GuardDuty Amazon-Kontingente

Ihr AWS-Konto Land verfügt über Standardkontingente, die früher als Limits bezeichnet wurden AWS-Service. Sofern nicht anders angegeben, gilt für jedes Kontingent Region-specific. Sie können Erhöhungen für einige Kontingente beantragen und andere Kontingente können nicht erhöht werden.

Um die Kontingente für anzuzeigen GuardDuty, öffnen Sie die Konsole Service Quotas. Wählen Sie im Navigationsbereich Amazon aus AWS-Servicesund wählen Sie es aus GuardDuty.

Informationen zur Erhöhung eines Kontingents finden Sie unter Anfordern einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch.

Ihr AWS-Konto hat die folgenden Kontingente für Amazon GuardDuty pro Region.

> **Note**
>
> - Spezifische Kontingente für GuardDuty Malware Protection for EC2 finden Sie unterKontingente im Malware-Schutz für EC2.
> - Spezifische Kontingente für Malware Protection for S3 finden Sie unterKontingente im Malware-Schutz für S3.

GuardDuty Kontingente pro Region

Ressource	Standard	Kommentare
Detektoren	1	Die maximale Anzahl an Detektorr essourcen, die Sie pro AWS -Konto und Region erstellen können. Sie können keine Erhöhung des Kontingents beantragen.

Ressource	Standard	Kommentare
Filter	100	Die maximale Anzahl an gespeicherten Filtern pro AWS Konto und Region. Sie können keine Erhöhung des Kontingents beantragen.
Aufbewahrungszeitraum für Ergebnisse	90 Tage	Die maximale Anzahl von Tagen, die ein Ergebnis aufbewahrt wird. Sie können keine Erhöhung des Kontingents beantragen.
IP-Adressen und CIDR-Bereiche pro Liste vertrauenswürdiger IP-Adressen	2.000	Die maximale Anzahl von IP-Adressen und CIDR-Bereichen, die Sie in eine einzige Liste vertrauen swürdiger IP-Adress en aufnehmen können. Sie können keine Erhöhung des Kontingents beantragen.

Ressource	Standard	Kommentare
IP-Adressen und CIDR-Bereiche pro Bedrohungsliste	250 000	Die maximale Anzahl von IP-Adressen und CIDR-Bereichen, die Sie in eine Liste mit Bedrohungsadressen aufnehmen können. Sie können keine Erhöhung des Kontingents beantragen.
Liste der Entitäten pro Bedrohungsentität	1.000	Die maximale Anzahl von Entitäten, die Sie in eine einzelne Liste von Bedrohung sentitäten aufnehmen können. Sie können keine Erhöhung des Kontingents beantragen.
Entitäten pro Liste vertrauenswürdiger Entitäten	1.000	Die maximale Anzahl von Entitäten, die Sie in eine Liste vertrauen swürdiger Entitäten aufnehmen können. Sie können keine Erhöhung des Kontingents beantragen.

Ressource	Standard	Kommentare
Maximale Dateigröße	35 MB	Die maximale Dateigröße für die Datei, die zum Hochladen einer Entitätsliste oder einer IP-Adressliste verwendet wird. Sie können keine Erhöhung des Kontingents beantragen.
Mitgliedskonten (nach Einladung)	5000	Die maximale Anzahl von Mitglieds konten, die mit einem Hauptkonto verknüpft sind. Sie können keine Erhöhung des Kontingents beantragen.

Ressource	Standard	Kommentare
Mitgliedskonten	50 000	Die maximale Anzahl von Mitglieds konten, die mit einem Administratorkonto durch AWS Organizat ions verknüpft sind. Dazu gehören auch Mitgliedskonten, die der Organisation auf Einladung hinzugefügt werden. Dieser Standardw ert hängt von Ihrem aktuellen Kontingen t für Mitgliedskonten in ab AWS Organizat ions. Die Anzahl der Mitgliedskonten GuardDuty , über AWS Organizat ions die hinzugefü gt werden, darf die Anzahl der Mitgliedskonten in Ihrer Organisation nicht überschreiten. Informationen zur Anzahl von AWS-Konten in einer Organisation finden Sie unter Höchst- und Mindestwerte im

Ressource	Standard	Kommentare
		AWS Organizations Benutzerhandbuch.
Informationssätze zu Bedrohungen (IP-Adressliste)	6	Die maximale Anzahl von Bedrohungs-IP-Adresslisten, die Sie AWS-Konto pro Region hinzufügen können. Sie können keine Erhöhung des Kontingents beantragen.
Vertrauenswürdige IP-Sets (IP-Adressliste)	1	Die maximale Anzahl vertrauenswürdiger IP-Adresslisten, die AWS-Konto pro Region hochgeladen und aktiviert werden können. Sie können keine Erhöhung des Kontingents beantragen.

Ressource	Standard	Kommentare
Listen bedrohlicher Entitäten	6	Die maximale Anzahl von Listen mit Bedrohungsentitäten, die Sie AWS-Konto pro Region hinzufügen können. Sie können keine Erhöhung des Kontingents beantragen.
Liste vertrauenswürdiger Entitäten	1	Die maximale Anzahl von Listen vertrauenswürdiger Entitäten, die AWS-Konto pro Region hochgeladen und aktiviert werden können. Sie können keine Erhöhung des Kontingents beantragen.

GuardDuty Support für verwaltete Instanzen

In der folgenden Tabelle GuardDuty ist die Unterstützung aufgeführt, die die verschiedenen Funktionen für die verschiedenen Arten von verwalteten Instances bieten.

Typ der verwalteten Funktion	Unterstützung für Runtime Monitoring	Malware-Schutz für EC2-Unterstützung
Amazon EKS Auto Mode	Unterstützt	Unterstützt
AWS Fargate Verwaltete Amazon ECS-Instanz	Nicht unterstützt	Unterstützt
Verwaltete Lambda-Instanz	Nicht unterstützt	Nicht unterstützt

Problembehebung bei Amazon GuardDuty

Wenn Sie Probleme im Zusammenhang mit der Durchführung einer bestimmten Aktion von haben GuardDuty, lesen Sie die Themen in diesem Abschnitt.

Topics

- Ergebnisse nach Amazon S3 exportieren — Zugriffsfehler
- Malware-Schutz bei EC2-Problemen
- Probleme mit der Laufzeitüberwachung
- Fehlerbehebung bei anderen Problemen

Ergebnisse nach Amazon S3 exportieren — Zugriffsfehler

Wenn Sie GuardDuty Ergebnisse in einen Amazon S3 S3-Bucket (Veröffentlichungsziel) exportieren und nicht auf dieses Veröffentlichungsziel zugreifen können, GuardDuty wird möglicherweise ein Zugriffsfehler angezeigt.

Wenn GuardDuty Sie die Einstellungen für den Export von Ergebnissen konfiguriert haben und die Ergebnisse nicht exportiert werden können, wird auf der Seite Einstellungen in der GuardDuty Konsole eine Fehlermeldung angezeigt. Dies kann möglicherweise passieren, wenn auf die Zielressource nicht mehr zugegriffen werden GuardDuty kann. Zum Beispiel, wenn Ihr Amazon S3 S3-Bucket gelöscht wurde oder die Zugriffsberechtigung für den Bucket geändert wurde. Dies kann möglicherweise auch passieren, wenn GuardDuty Sie nicht mehr auf den AWS KMS Schlüssel zugreifen können, der zur Verschlüsselung der Daten in Ihrem Amazon S3 S3-Bucket verwendet wurde. Wenn der Export nicht möglich GuardDuty ist, sendet es eine Benachrichtigung an die mit dem Konto verknüpfte E-Mail-Adresse mit Informationen zu diesem Problem.

Wie behebt man den Zugriffsfehler?

Um das Problem zu beheben, stellen Sie sicher, dass die entsprechenden Ressourcen vorhanden sind und GuardDuty über die erforderlichen Zugriffsrechte verfügen.

Weitere Informationen finden Sie unter Generierte Ergebnisse nach Amazon S3 exportieren.

Was passiert, wenn Sie diesen Fehler nicht beheben?

Wenn Sie das Problem nicht vor Ablauf der 90-tägigen Aufbewahrungsfrist für Ergebnisse lösen GuardDuty, werden Ihre Ergebnisse nicht exportiert. GuardDuty deaktiviert die Suche nach Exporteinstellungen für dieses Konto in der jeweiligen Region.

Um erneut mit dem Export der Ergebnisse zu beginnen, aktualisieren Sie die Konfigurationseinstellungen in der jeweiligen Region.

Malware-Schutz bei EC2-Problemen

In diesem Abschnitt werden die Fehler aufgeführt, die bei der Einrichtung oder Verwendung von Malware Protection for EC2 auftreten können.

Bei der Aktivierung des GuardDuty-initiated Malware-Scans fehlt die erforderliche AWS Organizations Verwaltungsberechtigung

Wenn Sie mehrere Konten mithilfe von verwalten möchten AWS Organizations und dieser Fehler angezeigt wird`The request failed because you do not have required AWS Organization master permission.`, fehlt Ihnen die Berechtigung, den GuardDuty-initiated Malware-Scan für mehrere Konten in Ihrer Organisation zu aktivieren.

Informationen zur Erteilung von Berechtigungen für das Verwaltungskonto finden Sie unterEinrichtung eines vertrauenswürdigen Zugriffs zur Aktivierung des GuardDuty-initiated Malware-Scans.

Ich initiiere einen On-demand Malware-Scan, der jedoch zu einem Fehler wegen fehlender erforderlicher Berechtigungen führt.

Wenn Sie eine Fehlermeldung erhalten, die darauf hindeutet, dass Sie nicht über die erforderlichen Berechtigungen verfügen, um einen On-demand Malware-Scan auf einer Amazon EC2 EC2-Instance zu starten, überprüfen Sie, ob Sie die AWS verwaltete Richtlinie: AmazonGuardDutyFullAccess_v2 (empfohlen) Richtlinie mit Ihrer IAM-Rolle verknüpft haben.

Wenn Sie Mitglied einer AWS Organisation sind und immer noch dieselbe Fehlermeldung erhalten, stellen Sie eine Verbindung mit Ihrem Verwaltungskonto her. Weitere Informationen finden Sie unter AWS Organizations SCP — Zugriff verweigert.

Ich erhalte bei der Arbeit mit Malware Protection for EC2 eine **`iam:GetRole`** Fehlermeldung.

Wenn Sie diesen Fehler — erhaltenUnable to get role: AWSServiceRoleForAmazonGuardDutyMalwareProtection, bedeutet das, dass Sie nicht berechtigt sind, entweder den Malware-Scan zu aktivieren oder den GuardDuty-initiated Malware-Scan zu verwenden On-demand . Stellen Sie sicher, dass Sie die AWS verwaltete Richtlinie: AmazonGuardDutyFullAccess_v2 (empfohlen)-Richtlinie Ihrer IAM-Rolle angehängt haben.

Ich habe ein GuardDuty Administratorkonto, das den GuardDuty-initiated Malware-Scan aktivieren muss, aber nicht die AWS verwaltete Richtlinie verwendet: AmazonGuardDutyFullAccess zur Verwaltung GuardDuty.

- Konfigurieren Sie die IAM-Rolle, die Sie mit GuardDuty verwenden, so, dass Sie über die erforderlichen Berechtigungen zum Aktivieren des GuardDuty-initiated Malware-Scans verfügen. Weitere Informationen zu den erforderlichen Berechtigungen finden Sie unter Eine serviceverknüpfte Rolle für Malware Protection for EC2 erstellen.
- Fügen Sie die AWS verwaltete Richtlinie: AmazonGuardDutyFullAccess_v2 (empfohlen) an Ihre IAM-Rolle an. Auf diese Weise können Sie den GuardDuty-initiated Malware-Scan für die Mitgliedskonten aktivieren.

Probleme mit der Laufzeitüberwachung

In diesem Abschnitt werden die Fehler aufgeführt, die bei der Einrichtung oder Verwendung von Runtime Monitoring auftreten können.

Probleme mit der Runtime-Abdeckung

Wenn die Runtime-Abdeckung Ihrer geschützten Ressourcen nicht mehr funktionsfähig ist, gibt die GuardDuty Konsole den genauen Problemtyp an. Nachdem Sie den Problemtyp ermittelt haben, können Sie sich anhand der folgenden Dokumente die Schritte zur Problembehandlung für jeden unterstützten Ressourcentyp ansehen:

- Behebung von Problemen mit der Amazon EC2-Laufzeitabdeckung
- Behebung von Problemen mit der ECS-Fargate Amazon-Laufzeitabdeckung
- Behebung von Problemen mit der Amazon EKS-Laufzeitabdeckung

Fehlerbehebung bei Speichermangel in Runtime Monitoring (nur Amazon EC2-Support)

In diesem Abschnitt werden die Schritte zur Problembehebung beschrieben, wenn der Fehler „Nicht genügend Arbeitsspeicher“ auftritt, basierend auf dem Problem, den GuardDuty Security Agent manuell CPU- und Speicherlimit zu installieren.

Wenn der GuardDuty Agent aufgrund des `out-of-memory` Problems `systemd` beendet wird und Sie der Meinung sind, dass es sinnvoll ist, dem GuardDuty Agenten mehr Speicher zur Verfügung zu stellen, können Sie das Limit aktualisieren.

1. Öffnen `/lib/systemd/system/amazon-guardduty-agent.service` Sie mit der Root-Berechtigung.
2. Suchen Sie `MemoryLimit` nach und und aktualisieren Sie beide Werte. `MemoryMax`

   ```
   MemoryLimit=256M
   MemoryMax=256M
   ```

3. Starten Sie den GuardDuty Agenten nach dem Aktualisieren der Werte neu, indem Sie den folgenden Befehl verwenden:

   ```
   sudo systemctl daemon-reload
   sudo systemctl restart amazon-guardduty-agent
   ```

4. Führen Sie den folgenden Befehl aus, um den Status anzuzeigen.

   ```
   sudo systemctl status amazon-guardduty-agent
   ```

   In der erwarteten Ausgabe wird das neue Speicherlimit angezeigt:

   ```
   Main PID: 2540 (amazon-guardduty)
   Tasks: 16
   Memory: 21.9M (limit: 256.0M)
   ```

Mein AWS Step Functions Workflow schlägt unerwartet fehl

Wenn der GuardDuty Container zum Workflow-Fehler beigetragen hat, finden Sie weitere Informationen unterBehebung von Problemen mit der ECS-Fargate Amazon-Laufzeitabdeckung.

Wenn das Problem weiterhin besteht, führen Sie einen der folgenden Schritte aus, um zu verhindern, dass der Workflow aufgrund des GuardDuty Containers fehlschlägt:

- Fügen Sie das `false` Tag`GuardDutyManaged`: zum zugehörigen Amazon ECS-Cluster hinzu.
- Deaktivieren Sie die automatische Agentenkonfiguration für AWS Fargate (nur ECS) auf Kontoebene. Fügen Sie das Inclusion-Tag`GuardDutyManaged`: `true` zu dem zugehörigen Amazon ECS-Cluster hinzu, den Sie mit dem GuardDuty automatisierten Agenten weiter überwachen möchten.

Fehlerbehebung bei anderen Problemen

Wenn Sie kein geeignetes Szenario für Ihr Problem finden, sehen Sie sich die folgenden Optionen zur Fehlerbehebung an:

- Informationen zu allgemeinen IAM-Problemen beim Zugriff auf finden Sie https://console.aws.amazon.com/guardduty/unterFehlerbehebung Amazon GuardDuty Amazon-Identität und Zugriff.
- Informationen zu Authentifizierungs- und Autorisierungsproblemen beim Zugriff AWS AWS Console Home finden Sie unter Problembehandlung bei IAM.

GuardDuty Amazon-Regionen und Endpunkte

Informationen darüber, AWS-Regionen wo Amazon verfügbar GuardDuty ist, finden Sie unter GuardDuty Amazon-Endpunkte in der Allgemeine Amazon Web Services-Referenz.

Wir empfehlen Ihnen, alle unterstützten GuardDuty AWS-Regionen Optionen zu aktivieren. Auf diese Weise können GuardDuty auch in Regionen, die Sie nicht aktiv nutzen, Erkenntnisse über unbefugte oder ungewöhnliche Aktivitäten generiert werden. Auf diese Weise können GuardDuty auch AWS CloudTrail Ereignisse für die unterstützten Länder überwacht werden. Die Fähigkeit AWS-Regionen, Aktivitäten zu erkennen, die globale Dienste betreffen, ist eingeschränkt.

Region-specific Verfügbarkeit von Funktionen

Eine Liste mit regionalen Unterschieden, um die Verfügbarkeit von GuardDuty Funktionen zu spezifizieren.

Erweiterte filterbare Felder für und CreateFilter UpdateFilter

Die zusätzlichen filterbaren Felder für Unterdrückungsregeln und Filter sind nur in der AWS Partition () `aws` verfügbar. In anderen Partitionen können Sie weiterhin die von der Konsole unterstützten Felder verwenden.

ListFindings und APIs GetFindingsStatistics

Die ListFindingsAPIs GetFindingsStatisticsund haben ein temporäres `consoleOnly` Flag. Wenn Sie eine oder beide dieser APIs verwenden, bedeutet das `consoleOnly` Flag, dass die API Ergebnisse bis zu einer Höchstgrenze von 1000 abrufen kann.

Malware-Schutz für EC2

GuardDuty unterstützt die Malware-Schutz für EC2 Funktion in den AWS Dedicated Local Zones.

RDS Protection

RDS-Schutz wird in der Region Asien-Pazifik (Taipeh) (`ap-east-2`) nicht unterstützt.

RDS-Schutz wird in den AWS Dedicated Local Zones nicht unterstützt.

IAM-Suchtyp — CredentialAccess:IAMUser/CompromisedCredentials

Der CredentialAccess:IAMUser/CompromisedCredentials Findetyp wird in den folgenden Regionen nicht unterstützt.

AWS-Region	Regionscode
AWS GovCloud (US-West)	us-gov-west-1
AWS GovCloud (US-East)	us-gov-east-1
China (Beijing)	cn-north-1
China (Ningxia)	cn-northwest-1

IAM-Suchtyp — DefenseEvasion:IAMUser/BedrockLoggingDisabled

Der DefenseEvasion:IAMUser/BedrockLoggingDisabled Findetyp wird in der Region Asien-Pazifik (Hongkong) (`ap-east-1`) nicht unterstützt.

Suchtypen für KI-Schutz

Für Impact:IAMUser/AnomalousModelInvocation die Impact:IAMUser/CostHarvesting Findetypen sind Amazon Bedrock oder Amazon SageMaker AI erforderlich. In Fällen AWS-Regionen , in denen Amazon Bedrock nicht verfügbar ist, werden diese Findetypen nur anhand von Amazon SageMaker AI-Modellaufrufen GuardDuty generiert. Informationen zu den Regionen, in denen Amazon Bedrock verfügbar ist, finden Sie unter Amazon Bedrock unterstützt AWS-Regionen im Amazon Bedrock-Benutzerhandbuch.

Der Impact:IAMUser/PromptInjection.Direct Findetyp hängt von Amazon Bedrock Guardrails ab, das nicht überall verfügbar ist. AWS-Regionen Dieser Findetyp wird nur in den Regionen unterstützt, in denen Amazon Bedrock Guardrails verfügbar ist. Die aktuelle Liste finden Sie unter Unterstützte Regionen für Amazon Bedrock Guardrails im Amazon Bedrock-Benutzerhandbuch.

Allgemeine API-Unterstützung

Die folgenden APIs in der Amazon GuardDuty API-Referenz können regionale Unterschiede aufweisen, da einige der zuvor angegebenen AWS-Regionen Datenquellen oder Funktionen nicht verfügbar sind:

- CreateDetector
- UpdateDetector
- UpdateMemberDetectors
- UpdateOrganizationConfiguration
- GetDetector

- GetMemberDetectors
- DescribeOrganizationConfiguration

Amazon-EC2-Erkenntnistypen – DefenseEvasion:EC2/UnusualDoHActivity und DefenseEvasion:EC2/UnusualDoTActivity

Die folgende Tabelle zeigt, AWS-Regionen wo verfügbar GuardDuty ist, aber diese beiden Amazon EC2-Suchttypen werden noch nicht unterstützt.

AWS-Region	Regionscode
Asien-Pazifik (Seoul)	ap-northeast-2
Asia Pacific (Osaka)	ap-northeast-3
Asien-Pazifik (Jakarta)	ap-southeast-3

AWS GovCloud (US) Regionen

Aktuelle Informationen finden Sie unter Amazon GuardDuty im AWS GovCloud (US) Benutzerhandbuch.

Regionen in China

Aktuelle Informationen finden Sie unter Verfügbarkeit von Features und Unterschiede bei der Implementierung.

GuardDuty ältere Aktionen und Parameter

Amazon GuardDuty hat einige API-Aktionen und -Parameter als veraltet eingestuft, unterstützt sie aber weiterhin. Es hat sich bewährt, die neuen API-Aktionen und -Parameter zu verwenden, die die alten Optionen ersetzen. Die folgende Tabelle vergleicht die alten und neuen Aktionen und Parameter.

Vermächtnis actions/parameters	Neu actions/parameters	Vergleich
DisassociateFromMasterAccount	DisassociateFromAdministratorAccount	Bei derselben Implementierung in beiden Aktionen GuardDuty wird der Begriff `Administrator` in verwendet`DisassociateFromAdministratorAccount` .
`autoEnable` Parameter in DescribeOrganizationConfigurationund UpdateOrganizationConfiguration	`autoEnableOrganizationMembers`	Mit `autoEnableOrganizationMembers` kann das GuardDuty Administratorkonto GuardDuty für alle Mitgliedskonten einen der Werte prüfen und durchsetzen. Bei der Verwendung von APIs kann die Aktualisierung der Konfiguration aller Mitgliedskonten bis zu 24 Stunden dauern. Weitere Informationen zu den möglichen Werten des `autoEnableOrganizationMembers` Feldes finden Sie unter autoEnableOrganizationMembers
`dataSources` -Parameter in den APIs, die in GuardDuty API-Änderungen	`features`	Ab März 2023 können Sie die neuen GuardDuty Schutzpläne konfigurieren GuardDuty Malware-Schutz für EC2 und verwenden`features`. Die vor März 2023 eingeführten Schutzplä

Vermächtnis actions/parameters	Neu actions/parameters	Vergleich
im März 2023 aufgeführt sind.		ne, einschließlich Malware Protection for EC2, unterstützen weiterhin die Konfiguration mithilfe von `dataSources` . Wenn Sie APIs verwenden, um einen Schutzplan zu konfigurieren, kann jede API-Anfrage entweder `dataSources` oder `features` beinhalten, aber nicht beide.

Dokumentenverlauf für Amazon GuardDuty

In der folgenden Tabelle werden wichtige Änderungen an der Dokumentation seit der letzten Veröffentlichung des GuardDuty Amazon-Benutzerhandbuchs beschrieben. Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Aktualisierte Funktionalität — Runtime Monitoring	GuardDuty Runtime Monitoring veröffentlicht die neue Security Agent-Version 1.16.0 für Amazon EKS-, Amazon EC2- und Amazon ECS-Ressourcen.AWS Fargate Weitere Informationen zur neuen Agent-Version und eine Liste zusätzlicher Ressourcen zur Aktualisierung Ihres Security Agents finden Sie unter Release-Versionen des GuardDuty Security Agents.	17. Juli 2026
Neuer Befundtyp — UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.InsideAWS und aktualisierter Befundtyp — UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS	GuardDuty führt einen neuen Suchtyp ein, der erkennt, wenn temporäre AWS Anmeldeinformationen, die für eine Amazon ECS-Aufgabe erstellt wurden, von einer anderen verwendet werden AWS-Konto. Darüber hinaus erkennt das bestehende ResourceCredentialExfiltration.OutsideAWS Ergebnis jetzt zusätzlich zu Lambda die Exfiltration der Anmeldeinformationen für Amazon	15. Juli 2026

	ECS-Aufgaben. Weitere Informationen erhalten Sie unter UnauthorizedAccess :IAMUser/ResourceCredential Exfiltration.InsideAWS und UnauthorizedAccess:IAMUser/ ResourceCredentialExfiltrat ion.OutsideAWS.	
Neuer Schutzplan - GuardDuty AI Protection	GuardDuty AI Protection erkennt Bedrohungen für KI-Workloads, die Amazon Bedrock und Amazon SageMaker AI verwenden . Wenn Sie den KI-Schutz aktivieren, GuardDuty werden die AWS CloudTrail Datenerei gnisse dieser Dienste analysiert, um anomale Modellaufrufe, Cost-Harv esting-Angriffe und direkte Prompt-Injection-Versuche zu erkennen. Weitere Informati onen finden Sie unter KI-Schutz. GuardDuty	13. Juli 2026

Zusätzliche Bedrohungsdetails im EventBridge Amazon-Ereignisschema für Malware Protection for S3	Das Ergebnis des EventBridge Amazon-Ereignisses zum Objektscan von Malware Protection for S3 enthält jetzt zusätzliche Bedrohungsdetails. Zu den neuen Feldern gehören `sourceitemDetails` ,`hash`, und`itemPath`. Weitere Informationen finden Sie unter Ergebnis des S3-Objektscans.	7. Juli 2026

GuardDuty Untersuchung (Vorschau)	Amazon bietet AI-powered Untersuchungen GuardDuty jetzt in einer öffentlichen Vorschauversion an. Sie können Untersuchungen erstellen, um GuardDuty Ergebnisse und Konten automatisch zu analysieren. Innerhalb weniger Minuten erhalten Sie eine strukturierte Zusammenfassung mit einer Vertrauensbewertung, einer Klassifizierung der MITRE ATT&CK® -Technik und umsetzbaren Empfehlungen. Sie können Untersuchungen von der GuardDuty Konsole, der CLI, der API oder dem MCP-Server aus einleiten. AWS Die Vorschau ist in 10 Sprachen verfügbar AWS-Regionen: USA Ost (Nord-Virginia), USA Ost (Ohio), USA West (Oregon), Kanada (Zentral), Europa (Frankfurt), Europa (Irland), Europa (London), Europa (Paris), Europa (Stockholm) und Asien-Pazifik (Tokio). Weitere Informationen finden Sie unter GuardDuty Investigation.	22. Juni 2026
Amazon RDS für MariaDB und MySQL	Database Insights ist jetzt verfügbar.	11. Juni 2026

Aktualisierte Funktionalität — Malware-Schutz für S3	GuardDuty hat die Kontingente von Malware Protection for S3 für die maximale Anzahl von Dateien, die aus einem Archiv extrahiert und analysiert werden können, sowie für die maximale Anzahl verschachtelter Archive, die extrahiert werden können, erhöht. Weitere Informationen finden Sie unter Kontingente in Malware Protection for S3.	9. Juni 2026
Neue Findetypen für Runtime Monitoring - SensitiveFileModified	GuardDuty Runtime Monitoring führt 3 neue Erkennungstypen ein, die Sie darüber informieren, wenn eine sicherheitsrelevante Systemdatei auf einer Amazon EC2-Instance oder einem Container geändert wurde, sodass ein Gegner möglicherweise Persistenz erlangt, Rechte erweitert oder sich der Erkennung entziehen kann. Weitere Informationen finden Sie unter Persistence:Runtime/SensitiveFileModified, PrivilegeEscalation:Runtime/SensitiveFileModified und DefenseEvasion:Runtime/SensitiveFileModified.	2. Juni 2026

Aktualisierte Funktionalität — Suche nach Filterkriterien	Nicht unterstützte Felder wurden aus der Liste der Suchfilterkriterien entfernt. Weitere Informationen finden Sie unter Ergebnisse filtern in GuardDuty.	29. Mai 2026
Zwei Befundarten wurden entfernt	Die Typen PrivilegeEscalation:Kubernetes/PrivilegedContainer und Persistence:Kubernetes/ContainerWithSensitiveMount Finding wurden entfernt.	29. Mai 2026
Aktualisierte Funktionalität — Runtime Monitoring	GuardDuty Runtime Monitoring Unterstützung für Kubernetes Version 1.36 hinzugefügt. Weitere Informationen finden Sie unter Voraussetzungen für die Laufzeitüberwachung.	28. Mai 2026
Aktualisierte Funktionalität — Runtime Monitoring	GuardDuty Runtime Monitoring veröffentlicht die neue Security Agent-Version 1.15.0 für Amazon ECS-Ressourcen.AWS Fargate Weitere Informationen zur neuen Agent-Version und eine Liste zusätzlicher Ressourcen zur Aktualisierung Ihres Security Agents finden Sie unter Release-Versionen des GuardDuty Security Agents.	28. Mai 2026

Aktualisierte Funktionalität — Erweiterte Bedrohung serkennung	GuardDuty Extended Threat Detection erweitert die Details zur Erkennung der Angriffssequenz um fünf neue Indikatortypen: MALICIOUS_PACKAGE, MISCONFIGURATION, REACHABILITY, SENSITIVE_DATA und VULNERABILITY. Weitere Informationen finden Sie unter Details zur Suche nach der Angriffssequenz. https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_findings-summary.html#guardduty-extended-threat-detection-attack-sequence-finding-details	20. Mai 2026
Aktualisierte Funktionalität — Runtime Monitoring	GuardDuty Runtime Monitoring veröffentlicht die neue Security Agent-Version 1.15.0 für Amazon EKS- und Amazon EC2-Ressourcen. Weitere Informationen zur neuen Agent-Version und eine Liste zusätzlicher Ressourcen zur Aktualisierung Ihres Security Agents finden Sie unter Release-Versionen des GuardDuty Security Agents.	14. Mai 2026

Aktualisiert AmazonGuardDutyServiceRolePolicy	Der `s3:ListBucket` `ecs:DescribeTasks` GuardDuty dienstverknüpften Rolle wurden, und `ecs:DescribeTaskDefinition` Berechtigungen hinzugefügt. Weitere Informationen finden Sie unter GuardDuty Aktualisierungen AWS verwalteter Richtlinien.	23. April 2026
Aktualisierte Funktionalität — Runtime Monitoring	GuardDuty Runtime Monitoring veröffentlicht die neue Security Agent-Version 1.12.2 für Amazon EKS-Ressourcen. Weitere Informationen zur neuen Agent-Version und eine Liste zusätzlicher Ressourcen zum Update Ihres Security Agents finden Sie unter GuardDuty Security Agent Release-Versionen.	22. April 2026
Aktualisierte Funktionalität — Erweiterte filterbare Felder	GuardDuty unterstützt jetzt das Filtern nach jedem Suchfeld, wenn Unterdrückungsregeln erstellt oder aktualisiert werden. Timestamp-Felder akzeptieren Werte im Unix-Epoch-Millisekundenformat. Weitere Informationen finden Sie unter Ergebnisse filtern in. GuardDuty	20. April 2026

Aktualisierte Funktionalität — Malware-Schutz für S3	Die EventBridge Benachrichtigung über die Ergebnisse der S3-Objektscans enthält jetzt ein `statusReasons` Feld, das angezeigt wird `scanResultDetails`, wenn ein Scan übersprungen wird. Dieses Feld enthält den spezifischen Grund, warum der Scan übersprungen wurde. Weitere Informationen finden Sie unter Status des potenziellen S3-Objekts und Ergebnisstatus.	10. April 2026
Aktualisierte Funktionalität — Runtime Monitoring	GuardDuty Runtime Monitoring veröffentlicht die neue Security Agent-Version 1.9.2 für Amazon EC2-Ressourcen. Weitere Informationen zu neuen Agentenversionen und eine Liste zusätzlicher Ressourcen zur Aktualisierung Ihres Security Agents finden Sie unter Release-Versionen des GuardDuty Security Agents.	3. April 2026

Aktualisiert AmazonGuardDutyServiceRolePolicy	Die `cloudtrail:CreateServiceLinkedChannel` Erlaubnis hinzugefügt, einen zusätzlichen Mechanismus zum Konsumieren von AWS CloudTrail Ereignissen zu aktivieren. Weitere Informationen finden Sie unter GuardDuty Aktualisierungen AWS verwalteter Richtlinien.	25. März 2026
Aktualisierte Funktionalität — Runtime Monitoring	GuardDuty Runtime Monitoring Unterstützung für Kubernetes Version 1.35 hinzugefügt. Weitere Informationen finden Sie unter Voraussetzungen für die Laufzeitüberwachung.	20. März 2026
Die neue Richtlinie `AmazonGuardDutyFullAccess_v2` mit eingeschränktem Geltungsbereich für vollen Zugriff ersetzt die Richtlinie `AmazonGuardDutyFullAccess`.	Mit Wirkung zum 13. März 2026 GuardDuty wurde die Richtlinie als veraltet eingestuft und durch eine `AmazonGuardDutyFullAccess` Richtlinie mit eingeschränktem Geltungsbereich mit dem Namen ersetzt. `AmazonGuardDutyFullAccess_v2` Weitere Informationen finden Sie unter Verwaltete Richtlinie: _v2. AWS AmazonGuardDutyFullAccess	13. März 2026

Neuer Befundtyp - CredentialAccess:IAMUser/CompromisedCredentials	GuardDuty Führt einen neuen Findetyp ein, der erkennt, wenn ein IAM-Zugriffsschlüssel, von dem festgestellt wurde, dass er potenziell kompromittiert wurde, zum Aufrufen von API-Vorgängen in verwendet wird. AWS Weitere Informationen finden Sie unter CredentialAccess:IAMUser/CompromisedCredentials.	6. März 2026
Neuer Befundtyp - UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS	GuardDuty führt einen neuen Suchtyp ein, der erkennt, wenn ein Host außerhalb von AWS versucht, AWS API-Operationen mit temporären AWS Anmeldeinformationen auszuführen, die für eine AWS Lambda Ressource in Ihrer AWS Umgebung erstellt wurden. Weitere Informationen finden Sie unter UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS.	16. Dezember 2025

Aktualisierte Funktionalität — Runtime Monitoring	GuardDuty Runtime Monitoring veröffentlicht die neue Security Agent-Version 1.9.1 für Amazon EC2-Ressourcen. Weitere Informationen zu neuen Agentenversionen und eine Liste zusätzlicher Ressourcen zur Aktualisierung Ihres Security Agents finden Sie unter Release-Versionen des GuardDuty Security Agents.	2. Dezember 2025
Aktualisierte Funktionalität — Runtime Monitoring	GuardDuty Runtime Monitoring veröffentlicht die neue Security Agent-Version 1.12.1 für Amazon EKS-Ressourcen. Weitere Informationen zur neuen Agent-Version und eine Liste zusätzlicher Ressourcen zur Aktualisierung Ihres Security Agents finden Sie unter GuardDuty Security Agent Release-Versionen.	2. Dezember 2025

Aktualisierte Funktionalität — Erweiterte Bedrohung serkennung	GuardDuty Extended Threat Detection führt zwei neue Typen zur Erkennung von Angriffssequenzen ein, mit AttackSequence:EC2/CompromisedInstanceGroup deren Hilfe mehrstufige Angriffe erkannt werden können AttackSequence:ECS/CompromisedCluster, an denen kompromittierte Amazon EC2-Instances und Amazon ECS-Cluster beteiligt sind. Aktivieren Sie Runtime Monitoring, um die Bedrohung serkennung zu maximieren. Weitere Informationen finden Sie unter Typen zur Suche nach Angriffssequenzen.	2. Dezember 2025
Neues Feature — Platzhalter in den Unterdrückungsregeln	GuardDuty hat seine Unterdrückungsfunktionen durch die Einführung von Übereinstimmungen und NotMatches Bedingungen, die Platzhalter unterstützen, erweitert. Kunden können jetzt * (um eine beliebige Anzahl von Zeichen abzugleichen) und? verwenden (um maximal einem Zeichen zu entsprech en) als Platzhalter bei der Erstellung von Unterdrüc kungsregeln. Unterdrüc kungsregeln.	2. Dezember 2025

Neue Funktion — Unterstützung für CloudWatch Amazon-Nutzungsmetriken	GuardDuty führt die Veröffentlichung von Nutzungsmetriken in Amazon CloudWatch für alle Schutzpläne ein, sodass Kunden die Nutzung überwachen können. Weitere Informationen finden Sie unter GuardDuty Nutzungsüberwachung und Kostenschätzung	25. November 2025
Neuer Befundtyp - DefenseEvasion:IAMUser/BedrockLoggingDisabled	GuardDuty führt einen neuen Findetyp ein, der erkennt, wenn die Protokollierung von Aufrufen des Amazon Bedrock-Modells deaktiviert ist. Dies könnte auf Versuche hindeuten, der Erkennung von KI-Workload-Aktivitäten zu entgehen. Weitere Informationen finden Sie unter DefenseEvasion:IAMUser/BedrockLoggingDisabled.	21. November 2025

Neue Funktion — Malware-Schutz für Backups	GuardDuty Malware Protection for Backup ist jetzt in allen kommerziellen Regionen verfügbar, in denen GuardDuty es verfügbar ist. Mit dieser Funktion können Sie das potenzielle Vorhandensein von Malware in Ihren Backup-Ressourcen durch vollständige und inkrementelle Scans von Amazon EBS-Snapshots, EC2-AMIs und Recovery Points erkennen. Weitere Informationen zu dieser Funktion finden Sie unter Malware-Schutz für Backups	19. November 2025
Wechseln Sie zu AmazonGuardDutyFullAccess und AmazonGuardDutyFullAccess_V2	Es wurde eine Berechtigung hinzugefügt, die es Ihnen ermöglicht, eine IAM-Rolle an diese zu übergeben, GuardDuty wenn Sie Malware Protection for Backup aktivieren.	19. November 2025

Neue Funktion — Malware-Schutz für S3-Scans auf Abruf.	GuardDuty kündigt Scan on Demand für Malware-Schutz für S3 an. Mit dieser Funktion können Sie die neue SendObjectMalwareScan API verwenden, um Scans für alle bereits vorhandenen Objekte auszulösen, die in Ihren S3-Buckets gespeichert sind. Weitere Informationen finden Sie unter S3-Malware-Scan https://docs.aws.amazon.com/guardduty/latest/ug/malware-protection-s3-on-demand.html auf Abruf.	17. November 2025
Aktualisierte Funktionalität — Runtime Monitoring	GuardDuty Runtime Monitoring veröffentlicht die neue Security Agent-Version 1.9.0 für Amazon AWS Fargate ECS-Ressourcen. Informationen zu neuen Agent-Versionen und eine Liste zusätzlicher Ressourcen zur Aktualisierung Ihres Security Agents finden Sie unter Release-Versionen des GuardDuty Security Agents.	28. Oktober 2025

Aktualisierte Funktionalität — Laufzeitüberwachung	GuardDuty Runtime Monitoring veröffentlicht die neue Security Agent-Version 1.9.0 für Amazon EC2-Ressourcen. Informationen zu neuen Agent-Versionen und eine Liste zusätzlicher Ressourcen zur Aktualisierung Ihres Security Agents finden Sie unter Release-Versionen des GuardDuty Security Agents.	23. Oktober 2025
Neuer Findetyp für Runtime Monitoring - DefenseEvasion:Runtime/KernelModuleLoaded	GuardDuty Runtime Monitoring führt einen neuen Erkennungstyp ein, der Ihnen hilft, Techniken zur Umgehung von Abwehrmaßnahmen zu identifizieren, bei denen Bedrohungsakteure Kernelmodule verwenden, um Sicherheitskontrollen zu umgehen, Systemabläufe zu ändern und dauerhaften Systemzugriff zu erhalten. Weitere Informationen finden Sie unter DefenseEvasion:Runtime/KernelModuleLoaded.	15. Oktober 2025

Aktualisierte Funktionalität — Runtime Monitoring	Unterstützung für Kubernetes-Version 1.34 für die Betriebssystemverteilungen und die Security Agent-Version für GuardDuty SageMaker Role Manager für Amazon EKS-Ressourcen hinzugefügt. Weitere Informationen finden Sie unter Überprüfen der Architekturanforderungen für Amazon EKS.	3. Oktober 2025
Eine Anleitung zur Fehlerbehebung bei Problemen mit der Amazon RDS-Datenbank wurde hinzugefügt	Es wurden Anleitungen zur Behebung von RDS-Datenbankproblemen hinzugefügt, die sich auf die Überwachungsfunktionen von GuardDuty RDS Protection auswirken können, einschließlich `storage-full` Status- und RDS for PostgreSQL-Read Replica-Anforderungen. Weitere Informationen finden Sie unter Problembehandlung bei der Überwachung von RDS Protection.	15. September 2025

Aktualisierte Funktionalität — Laufzeitüberwachung	Ubuntu Noble OS-Distribution mit Unterstützung für die Kernel-Versionen 6.13 und 6.14 für GuardDuty Runtime Monitoring für Amazon EC2 hinzugefügt. Informationen zur EC2-Agentenversion, die für diese Betriebssystemdistribution unterstützt wird, finden Sie unter Überprüfen der Architekturanforderungen für Amazon EC2.	13. September 2025
Aktualisierte Funktionalität — RDS Protection	PostgreSQL 17-Unterstützung für RDS für PostgreSQL-Datenbanken hinzugefügt, die von RDS Protection überwacht werden. GuardDuty Weitere Informationen finden Sie unter Unterstützte Datenbanken in RDS Protection.	13. September 2025
Aktualisierte Funktionalität — Malware-Schutz für S3	GuardDuty Malware Protection for S3 erhöht das Standardkontingent für entpackte Archivdateien von 1.000 auf 10.000 Dateien. Weitere Informationen finden Sie unter Kontingente in Malware Protection for S3.	3. September 2025

Aktualisierte Funktionalität — Runtime Monitoring	GuardDuty Runtime Monitoring veröffentlicht die neue Security Agent-Version 1.11 für Amazon EKS-Ressourcen. Weitere Informationen zur neuen Agent-Version und eine Liste zusätzlicher Ressourcen zur Aktualisierung Ihres Security Agents finden Sie unter Release-Versionen des GuardDuty Security Agents.	29. August 2025
Aktualisierte Funktionalität — Arbeiten mit Listen	GuardDuty führt benutzerdefinierte Listen vertrauenswürdiger und bedrohlicher Entitäten ein, die sowohl IP-Adressen als auch Domainnamen unterstützen. GuardDuty unterstützt weiterhin die IP-Adressliste und empfiehlt, die Entitätsliste für die benutzerdefinierte Bedrohungserkennung zu verwenden. Weitere Informationen finden Sie unter Anpassen der Bedrohungserkennung mit Entitätslisten und IP-Adresslisten.	15. August 2025

Aktualisierte Funktionalität — Runtime Monitoring	GuardDuty Runtime Monitoring veröffentlicht die neue Security Agent-Version 1.8.0 sowohl für Amazon EC2-AWS Fargate als auch für Amazon ECS-Ressourcen. Weitere Informationen zu neuen Agent-Versionen und eine Liste zusätzlicher Ressourcen zur Aktualisierung Ihres Security Agents finden Sie unter Release-Versionen des GuardDuty Security Agents.	12. August 2025
Unterstützung für die Region Asien-Pazifik (Taipeh)	Amazon GuardDuty ist jetzt in der Region Asien-Pazifik (Taipeh) (`ap-east-2`) verfügbar. Informationen zur Aktivierung GuardDuty in dieser Region finden Sie unter Erste Schritte. Sie können Benachrichtigungen über Aktualisierungen der GuardDuty Funktionen und Bedrohungserkennungen erhalten, indem Sie die GuardDuty Ankündigungen von Amazon SNS in dieser Region abonnieren.	31. Juli 2025

Aktualisierte Funktionalität — Malware-Schutz für S3	Malware Protection for S3 unterstützt jetzt das Scannen von Objekten bis zu 100 GB (vorher 5 GB). Dies umfasst sowohl einzelne Objekte als auch extrahierte Archivdat eien. Weitere Informationen finden Sie unter Malware-S chutz für S3-Kontingente.	23. Juli 2025
Aktualisierte Funktionalität — Erwarteter Bucket-Besitzer in den Vertrauenslisten zu IP- und Bedrohungslisten hinzugefügt	GuardDuty Das Feld Erwarteter Bucket-Besitzer für Listen mit vertrauenswürdigen IP-Adressen und Bedrohungs-IP-Adressen wurde hinzugefü gt. In diesem optionalen Feld können Sie eine AWS-Konto ID angeben, die zur Überprüfung der Inhabersc haft des Amazon S3-Bucket s verwendet GuardDuty wird. Weitere Informationen finden Sie unter Arbeiten mit Listen mit vertrauenswürdigen IP-Adressen und Bedrohung slisten.	16. Juli 2025

Aktualisierte Funktionalität — Erweiterte Bedrohung serkennung	GuardDuty Extended Threat Detection erweitert jetzt die Unterstützung für Amazon EKS-Cluster, indem mehrere Sicherheitssignale aus den EKS-Auditprotokollen, dem Laufzeitverhalten von Prozessen und der AWS API-Aktivität korreliert werden. Aktivieren Sie EKS Protectio n, Runtime Monitoring (mit EKS-Add-on) oder beides, um die Bedrohungserkennung zu maximieren. Zur Identifiz ierung potenzieller Bedrohung en GuardDuty wird ein neuer Erkennungstyp eingeführt — AttackSequence:EKS/ CompromisedCluster. Weitere Informationen finden Sie unter Erweiterte Bedrohung serkennung.	17. Juni 2025
Aktualisierte Funktionalität — Malware-Schutz für S3	Malware Protection for S3 unterstützt das Scannen von Archiven mit extrem hoher Komprimierungsrate nicht. Diese Dateien werden beim Scannen übersprungen und mit dem Scanergebnis von `UNSUPPORTED` markiert. Weitere Informationen finden Sie unter Status des potenziel len S3-Objekts und Ergebniss tatus.	13. Juni 2025

Aktualisierte Funktionalität — Malware-Schutz für EC2	Malware Protection for EC2 bietet zusätzliche Unterstützung für das Scannen der meisten Instanzen mit `productCode` as. `marketplace` Dies gilt sowohl für GuardDuty-initiated Malware-Scans als auch für On-demand Malware-Scans. Weitere Informationen finden Sie unter Gründe für das Überspringen von Ressourcen beim Malware-Scan.	13. Juni 2025
Neue AmazonGuardDutyFullAccess _v2-Richtlinie	Eine neue AmazonGuardDutyFullAccess_v2 Richtlinie mit Berechtigungen zur Erhöhung der Sicherheit wurde hinzugefügt, indem administrative Aktionen auf GuardDuty Dienstprinzipale beschränkt werden. Informationen zu dieser empfohlenen Richtlinie finden Sie unter AWS Verwaltete Richtlinie:. AmazonGuardDutyFullAccess_v2	4. Juni 2025

Erweiterte regionale Unterstützung für RDS Protection	GuardDuty RDS Protection ist jetzt in den Regionen Mexiko (Zentral), Asien-Pazifik (Thailand) und Asien-Pazifik (Malaysia) verfügbar. RDS Protection hilft Ihnen, potenziell verdächtiges Anmeldeverhalten in unterstützten Aurora MySQL, Aurora PostgreSQL (einschließlich Limitless Database) und RDS for PostgreSQL zu erkennen. GuardDuty Generiert im Falle einer Erkennung einer Bedrohung einen RDS-Schutzbefund. Weitere Informationen zu unterstützten Datenbanken und zur Aktivierung dieses Schutzplans in den neu unterstützten Regionen finden Sie unter RDS-Schutz.	4. Juni 2025
Aktualisierte Funktionalität — Runtime Monitoring	GuardDuty Runtime Monitoring veröffentlicht die neue Security Agent-Version 1.7.1 für Amazon EC2-Ressourcen. Weitere Informationen zu neuen Agentenversionen und eine Liste zusätzlicher Ressourcen zur Aktualisierung Ihres Security Agents finden Sie unter Release-Versionen des GuardDuty Security Agents.	3. Juni 2025

Unterstützung für erweiterte Bedrohungserkennung	GuardDuty Extended Threat Detection ist jetzt im asiatisch-pazifischen Raum (Thailand) verfügbar (ap-southeast-7). Ohne dass eine Aktivierung erforderlich ist, erkennt es mehrstufige Angriffe, die sich über Datenquellen, mehrere Arten von AWS Ressourcen und Zeit erstrecken — innerhalb eines. AWS-Konto Wenn potenzielle Bedrohungen erkannt werden, generiert es eine Suche nach der Angriffssequenz. Weitere Informationen finden Sie unter Erweiterte Bedrohungserkennung.	12. Mai 2025
Unterstützung für die Region Mexiko (Zentral)	Amazon GuardDuty ist jetzt in der Region Mexiko (Zentral) (`mx-central-1`) verfügbar. Informationen zur Aktivierung GuardDuty in dieser Region finden Sie unter Erste Schritte. Sie können Benachrichtigungen über Aktualisierungen der GuardDuty Funktionen und Bedrohungserkennungen erhalten, indem Sie die GuardDuty Ankündigungen von Amazon SNS in dieser Region abonnieren.	7. Mai 2025

Aktualisierte Funktionalität — Laufzeitüberwachung	GuardDuty Runtime Monitoring veröffentlicht die neue Security Agent-Version 1.10.0 für Amazon EKS-Ressourcen. Weitere Informationen zu neuen Agent-Versionen und eine Liste zusätzlicher Ressourcen zur Aktualisierung Ihres Security Agents finden Sie unter Release-Versionen des GuardDuty Security Agents.	4. April 2025
Aktualisierte Funktionalität — Runtime Monitoring	GuardDuty Runtime Monitoring veröffentlicht die neue Security Agent-Version 1.7.0 für ECS-Fargate Amazon-Ressourcen. Weitere Informationen zu neuen Agent-Versionen und eine Liste zusätzlicher Ressourcen zur Aktualisierung Ihres Security Agents finden Sie unter Release-Versionen des GuardDuty Security Agents.	4. April 2025

Aktualisierte Funktionalität — Runtime Monitoring	GuardDuty Runtime Monitoring veröffentlicht die neue Security Agent-Version 1.7.0 für Amazon EC2-Ressourcen. Weitere Informationen zu neuen Agentenversionen und eine Liste zusätzlicher Ressourcen zur Aktualisierung Ihres Security Agents finden Sie unter Release-Versionen des GuardDuty Security Agents.	3. April 2025
Unterstützung für die Region Asien-Pazifik (Thailand)	Amazon GuardDuty ist jetzt in der Region Asien-Pazifik (Thailand) verfügbar. Informationen darüber, welche Funktionen in dieser Region unterstützt werden, finden Sie unter Verfügbarkeit von Region-specific Funktionen. Informationen zur Aktivierung GuardDuty in dieser Region finden Sie unter Erste Schritte. Sie können Benachrichtigungen über Aktualisierungen der GuardDuty Funktionen und Bedrohungserkennungen erhalten, indem Sie die Ankündigungen von Amazon GuardDuty SNS abonnieren.	1. April 2025

Aktualisierte Funktionalität	Das Übersichts-Dashboard zeigt jetzt Erkenntnisse, die auf allen generierten Sicherheitsergebnissen basieren, wodurch die vorherige Beschränkung auf 5.000 Ergebnisse aufgehoben wurde. Informationen zu diesen Erkenntnissen finden Sie unter GuardDuty Übersichts-Dashboard.	17. März 2025
Aktualisierte Funktionalität — Laufzeitüberwachung	GuardDuty Runtime Monitoring veröffentlicht die neue Security Agent-Version 1.9.0 für Amazon EKS-Ressourcen. Weitere Informationen zu neuen Agent-Versionen und eine Liste zusätzlicher Ressourcen zur Aktualisierung Ihres Security Agents finden Sie unter Release-Versionen des GuardDuty Security Agents.	2. März 2025
Aktualisierte Funktionalität — Runtime Monitoring	GuardDuty Runtime Monitoring hat einen neuen Coverage-Problemtyp (Agent Not Provisioned) für Amazon EC2-Ressourcen hinzugefügt. Informationen zur Behebung dieses Problems finden Sie unter Problembehandlung bei Problemen mit der Amazon EC2-Laufzeitabdeckung.	21. Februar 2025

Aktualisierte Funktionalität — Laufzeitüberwachung	GuardDuty Runtime Monitoring veröffentlicht neue Sicherheitsagenten für Amazon EC2- und ECS-Fargate Amazon-Ressourcen. Weitere Informationen zu neuen Agentenversionen und eine Liste zusätzlicher Ressourcen zur Aktualisierung Ihrer Security Agents finden Sie unter Release-Versionen der GuardDuty Security Agents.	6. Februar 2025
GuardDuty Unterstützung in der bestehenden Region Asien-Pazifik (Malaysia)	GuardDuty Extended Threat Detection ist jetzt in der Region Asien-Pazifik (Malaysia) verfügbar. Weitere Informationen finden Sie unter Erweiterte Bedrohungserkennung.	28. Januar 2025

Unterstützung für die Region Asien-Pazifik (Malaysia)	Amazon GuardDuty ist jetzt in der Region Asien-Pazifik (Malaysia) verfügbar. Informationen darüber, welche Funktionen in dieser Region unterstützt werden, finden Sie unter Verfügbarkeit von Region-specific Funktionen. Informationen zur Aktivierung GuardDuty in dieser Region finden Sie unter Erste Schritte. Sie können Benachrichtigungen über Aktualisierungen der GuardDuty Funktionen und Bedrohungserkennungen erhalten, indem Sie die Ankündigungen von Amazon GuardDuty SNS abonnieren.	16. Januar 2025
Aktualisierte Funktionalität — Runtime Monitoring	GuardDuty Runtime Monitoring hat zusätzliche Informationen und Schritte zur Behebung von Problemen mit der ECS-Fargate Amazon-Abdeckung aktualisiert, die mit einem nicht bereitgestellten Agenten zusammenhängen. Weitere Informationen zum Problemtyp „Agent nicht bereitgestellt“ finden Sie unter Problembehandlung bei Problemen mit der ECS-Fargate Amazon-Runtime-Abdeckung.	8. Januar 2025

Neuer Befundtyp - Policy:IAMUser/ShortTermRootCredentialUsage	GuardDuty führt einen neuen Suchtyp ein, der Sie warnt, wenn eingeschränkte Benutzeranmeldeinformationen, die für die AWS-Konten in Ihrer Umgebung aufgelisteten Benutzer erstellt wurden, für Anfragen verwendet werden AWS-Services. Weitere Informationen finden Sie unter Policy:IAMUser/ShortTermRootCredentialUsage.	8. Januar 2025
Neue Funktion — GuardDuty Erweiterte Bedrohungserkennung	GuardDuty kündigt Extended Threat Detection an, um mehrstufige Angriffssequenzen zu erkennen, die sich über einen bestimmten Zeitraum auf GuardDuty grundlegende Datenquellen und AWS Ressourcen in Ihrem AWS-Konto Unternehmen erstrecken. Ohne zusätzliche Kosten wird diese Funktion automatisch für alle Konten aktiviert, die aktiviert wurden. GuardDuty Diese Funktion kündigt zwei neue GuardDuty Erkennungstypen an, die als Typen zur Suche nach Angriffssequenzen bezeichnet werden. Weitere Informationen finden Sie unter Erweiterte Bedrohungserkennung.	01. Dezember 2024

Verbesserte dienstübergreifende Funktionalität — Runtime Monitoring und Malware-Schutz für EC2	Auswirkungen der neuen Funktionen von Amazon Elastic Kubernetes Service (Amazon EKS) auf Amazon-Funktionen: GuardDuty • Amazon EKS Auto Mode — Sowohl Runtime Monitoring für Amazon EKS als auch Malware Protection für EC2 unterstützen dies. • Amazon EKS-Hybridknoten — Sowohl Runtime Monitoring für Amazon EKS als auch Malware Protection for EC2 unterstützen dies nicht. Weitere Informationen finden Sie unter So funktioniert Runtime Monitoring mit Amazon EKS-Clustern und Malware-Schutz für EC2.	01. Dezember 2024

Aktualisierte Funktionen in Runtime Monitoring — Amazon EKS	Runtime Monitoring hat eine neue Agentenversion 1.8.1 (v1.8.1-eks-build.2) für Amazon EKS-Resso urcen veröffentlicht. Mit dieser neuen Agentenversion wird die Runtime Monitorin g-Unterstützung für Amazon EKS-Ressourcen GuardDuty erweitert, die auf CentOS und Fedora ausgeführt werden. RedHat Weitere Informationen finden Sie unter Validierung der Architekturanforderungen. Informationen zu Versionsh inweisen finden Sie unter GuardDuty Security Agent für Amazon EKS-Ressourcen.	23. November 2024
Aktualisierte Funktionalität in Runtime Monitoring — Amazon EC2	Runtime Monitoring hat eine neue Agentenversion 1.5.0 für Amazon EC2-Ressourcen veröffentlicht. Mit dieser neuen Agentenversion wird die Runtime Monitoring-Unterstützung für Amazon EC2-Ressourcen GuardDuty erweitert, die auf CentOS und RedHat Fedora ausgeführt werden. Weitere Informationen finden Sie unter Validierung der Architekturanforderungen. Informationen zu Versionsh inweisen finden Sie unter GuardDuty Security Agent für Amazon EC2-Ressourcen.	20. November 2024

Aktualisierte Funktionalität in Runtime Monitoring — Amazon ECS-Fargate	Runtime Monitoring hat eine neue Agentenversion 1.5.0 für ECS-Fargate Amazon-Ressourcen veröffentlicht. Weitere Informationen zu Versionshinweisen finden Sie unter GuardDuty Security Agent für AWS Fargate (nur Amazon ECS).	14. November 2024
Die Funktionalität von Malware Protection for EC2 wurde aktualisiert	GuardDuty Malware Protection for EC2 hat der Liste der Ergebnisse, die einen GuardDuty-initiated Malware-Scan auf Amazon EC2-Instances auslösen, drei Erkennungstypen für Runtime Monitoring hinzugefügt. Konten, die Malware Protection for EC2 aktiviert haben, beobachten den GuardDuty-initiated Malware-Scan, wenn eines der folgenden GuardDuty Ergebnisse generiert wird: • Execution:Runtime/MaliciousFileExecuted • Execution:Runtime/SuspiciousShellCreated • PrivilegeEscalation:Runtime/ElevationToRoot	7. November 2024

Aktualisierte Funktionen in RDS Protection	GuardDuty RDS Protection fügt der Liste der unterstützten Datenbanken die neu veröffentlichte Aurora PostgreSQL Limitless Database Engine-Version `16.4-limitless` hinzu. Wenn Sie RDS Protection bereits aktiviert haben, GuardDuty wird automatisch damit begonnen, das Anmeldeverhalten für die Limitless Database zu überwachen. AWS-Konten Für Konten, die die kostenlose 30-Tage-Testversion von RDS Protection bereits genutzt haben, fallen Nutzungskosten für Limitless Database sowie für andere unterstützte Datenbanken an, die überwacht werden. Weitere Informationen finden Sie unter RDS Protection. https://docs.aws.amazon.com/guardduty/latest/ug/rds-protection.html	6. November 2024

Regionserweiterung - GuardDuty und AWS PrivateLink Integration	GuardDuty erweitert jetzt die Regionsunterstützung für Amazon GuardDuty und die Schnittstelle VPC-Endpunkte ()AWS PrivateLink. Zuvor war die Regionsunterstützung für die USA Ost (Nord-Virginia), Europa (Irland) und Israel (Tel Aviv) verfügbar. Diese Unterstützung wird jetzt auf alle Bereiche ausgedehnt, AWS-Regionen in denen sie verfügbar GuardDuty ist. Weitere Informationen zu regionalen Unterschieden finden Sie unter Verfügbarkeit von Region-specific Funktionen.	6. November 2024
Aktualisierte Funktionalität in Runtime Monitoring — Amazon ECS-Fargate	Runtime Monitoring hat eine neue Agentenversion 1.4.1 für ECS-Fargate Amazon-Ressourcen veröffentlicht. Weitere Informationen zu Versionshinweisen finden Sie unter GuardDuty Security Agent für AWS Fargate (nur Amazon ECS).	24. Oktober 2024

Unterstützung für GuardDuty CloudFormation Tag-Operationen hinzugefügt	GuardDuty unterstützt jetzt die Aktualisierung von Tag-Schlüsseln und -Werten sowie von Tags auf Stack-Ebene. Dazu fügen Sie der IAM-Rolle die Berechtigung `guardduty:tagResource` hinzu. Weitere Informationen dazu GuardDuty CloudFormation finden Sie in der Referenz zum GuardDuty Amazon-Ressourcentyp im AWS CloudFormation Benutzerhandbuch.	24. Oktober 2024
Aktualisierte Funktionalität im GuardDuty Malware-Schutz für S3	Wenn Sie den Malware-Schutz für S3 aktivieren, können Sie eine Servicerolle auswählen, die über die erforderlichen Berechtigungen verfügt, um in Ihrem Namen Malware-Scanaktionen durchzuführen. Weitere Informationen zur Aktivierung des Malware-Schutzes für S3 finden Sie unter Konfiguration des Malware-Schutzes für S3 für Ihren S3-Bucket.	22. Oktober 2024

Aktualisierte Funktionalität	GuardDuty erweitert den UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS Suchtyp, um die Verwendung von Amazon AWS EC2-Instance-Anmeldeinformationen von VPC-Endpunkten (AWS PrivateLink) zu erkennen AWS-Konten , die nicht mit der Amazon EC2-Instance-Rolle verknüpft sind. Diese neue GuardDuty Funktion erkennt potenziellen Missbrauch von Amazon EC2-Instance-Anmeldeinformationen und liefert den Kontext, in dem die AWS-Konto Remote-Daten der ausreisenden Sitzung verwendet werden. Weitere Informationen zu AWS Service-Endpunkten, die von dieser neuen Erkennung unterstützt werden, finden Sie im Benutzerhandbuch unter Protokollieren von Netzwerkaktivitätsereignissen. AWS CloudTrail	21. Oktober 2024

Aktualisierte Funktionalität — GuardDuty Runtime Monitoring	GuardDuty Runtime Monitoring hat die folgenden drei Erkennungstypen hinzugefügt, die Sie benachrichtigen, wenn verdächtige Befehle auf einer Amazon EC2-Instance oder einem Container-Workload in Ihrer AWS Umgebung ausgeführt werden: • Discovery:Runtime/SuspiciousCommand • Persistence:Runtime/SuspiciousCommand • PrivilegeEscalation:Runtime/SuspiciousCommand	10. Oktober 2024
Neue Funktion - Unterstützung für VPC-Endpunkte hinzugefügt	GuardDuty ist jetzt in VPC-Endpunkte integriert AWS PrivateLink und unterstützt diese. Weitere Informationen zur AWS PrivateLink Integration finden Sie unter Amazon GuardDuty und unter Interface VPC Endpoints ().AWS PrivateLink	17. September 2024
Aktualisierte Funktionalität in Runtime Monitoring — Amazon EKS	Runtime Monitoring hat eine neue Agentenversion 1.7.1 für Amazon EKS-Ressourcen veröffentlicht. Weitere Informationen zu Versionshinweisen finden Sie unter GuardDuty Security Agent für Amazon EKS.	13. September 2024

Die Funktionalität von Malware Protection for S3 wurde aktualisiert	Malware Protection for S3 hat ein neues Feld zum Amazon EventBridge (EventBridge) - Schema für das Ergebnis des S3-Objektscans hinzugefügt. `s3Throttled` Das `s3Throttled` Feld gibt an, ob es beim Hoch- oder Abrufen von Speicher aus Amazon Simple Storage Service (Amazon S3) - Buckets zu einer Verzögerung gekommen ist. Weitere Informationen finden Sie unter Überwachen von S3-Objektscans mit Amazon. EventBridge	13. September 2024
Aktualisierte Funktionalität in Runtime Monitoring — Amazon EC2	Runtime Monitoring hat eine neue Agentenversion 1.3.1 für Amazon EC2-Ressourcen veröffentlicht. Weitere Informationen zu Versionshinweisen finden Sie unter GuardDuty Security Agent für Amazon EC2.	12. September 2024
Aktualisierte Funktionalität in Runtime Monitoring — Amazon ECS-Fargate	Runtime Monitoring hat eine neue Agentenversion 1.3.1 für ECS-Fargate Amazon-Ressourcen veröffentlicht. Weitere Informationen zu Versionshinweisen finden Sie unter GuardDuty Security Agent für AWS Fargate (nur Amazon ECS).	11. September 2024

Die GuardDuty service-verknüpfte Rolle (SLR) wurde aktualisiert	GuardDuty hat die SLR aktualisiert, um die `ec2:Describe:Vpcs` Berechtigung in die Amazon EC2-Aktionen aufzunehmen. Weitere Informationen finden Sie unter Service-linked Rollenberechtigungen für. GuardDuty	22. August 2024
Signifikante Erweiterung des Inhalts	GuardDuty der Funktion „Malware-Schutz für S3“ wurden wichtige Inhaltsaktualisierungen hinzugefügt. • Es wurden neue Beispiele für ein Beispiel-Benachrichtigungsschema hinzugefügt, um EventBridge Amazon-Regeln für den Empfang von Benachrichtigungen im Zusammenhang mit dem Ressourcenstatus des Malware-Schutzplans und den Ergebnissen des S3-Objektscans einzurichten. Weitere Informationen finden Sie unter Überwachen von S3-Objektscans mit Amazon EventBridge. • Es wurden Informationen zur Behebung von Tagfehlern nach dem Scannen von S3-Objekten hinzugefügt.	20. August 2024

Aktualisierte Funktionalität in GuardDuty Runtime Monitoring — Amazon EC2	Runtime Monitoring hat eine neue Agentenversion 1.3.0 für Amazon EC2-Ressourcen veröffentlicht. Weitere Informationen zu Versionshinweisen finden Sie unter GuardDuty Security Agent für Amazon EC2.	19. August 2024
Aktualisierte Funktionalität in GuardDuty Runtime Monitoring — Amazon EKS	Runtime Monitoring hat eine neue Agentenversion 1.7.0 für Amazon EKS-Ressourcen veröffentlicht. Weitere Informationen zu Versionshinweisen finden Sie unter GuardDuty Security Agent für Amazon EKS-Cluster.	17. August 2024
Signifikante Ergänzung des Inhalts	GuardDuty hat neue Informationen zur Malware-Erkennungsmethode und zu den Scan-Engines hinzugefügt, die es für die Funktionen Malware Protection for S3 und Malware Protection for EC2 verwendet. Weitere Informationen finden Sie unter Scan Engine zur Erkennung von GuardDuty Schadsoftware.	15. August 2024

Neue Funktion - Schutz von KI-Workloads	GuardDuty Die grundlegende Bedrohungserkennung und Lambda Protection helfen Ihnen dabei, Bedrohungen für darauf aufbauende KI-Workloads besser abzusichern und zu erkennen. AWS Weitere Informationen finden Sie unter Schützen von KI-Workloads mit. GuardDuty	14. August 2024
Aktualisierte Funktionalität in GuardDuty Runtime Monitoring — Fargate (nur Amazon ECS)	Runtime Monitoring hat eine neue Agentenversion 1.3.0 für Ressourcen AWS Fargate (nur Amazon ECS) veröffentlicht. Weitere Informationen zu Versionshinweisen finden Sie unter GuardDuty Security Agent für Fargate-ECS.	9. August 2024
Aktualisierte Funktionalität — Malware-Schutz für S3	GuardDuty Malware Protection for S3 erhöht das Kontingent für die maximale Anzahl von S3-Buckets von 10 auf 25 Buckets. Dieses Kontingent gilt für jeweils ein Kontingent AWS-Konto . AWS-Region Weitere Informationen finden Sie unter Malware-Schutz für S3.	8. August 2024

Aktualisiert — Neue Suchtypen in Runtime Monitoring	GuardDuty hat zwei neue Erkennungstypen für Runtime Monitoring hinzugefügt, mit deren Hilfe Sie Bedrohungen erkennen können, die eine verdächtige Shell-Erstellung auf der überwachten Ressource beinhalten, und eine Rechteeskalation, bei der ein Prozess seine Rechte verdächtig auf root erhöht. • Execution:Runtime/SuspiciousShellCreated • PrivilegeEscalation:Runtime/ElevationToRoot	6. August 2024
Aktualisiert — Integration mit AWS Security Hub CSPM	AWS Security Hub CSPM bietet eine Liste von GuardDuty Sicherheitskontrollen, mit denen Sie Ihre Ressourcen bewerten und überprüfen können, ob Sie die Sicherheitsstandards und bewährten Verfahren der Sicherheitsbranche einhalten. Weitere Informationen finden Sie unter Verwenden von GuardDuty Kontrollen in Security Hub CSPM.	11. Juli 2024

Das GuardDuty Testskript für die Ergebnisse wurde aktualisiert	GuardDuty unterstützt jetzt über 100 Ergebnisse mit unterschiedlichen AWS Ressourcen in einem speziellen Konto. Weitere Informationen finden Sie unter GuardDuty Testergebnisse in speziellen Konten.	28. Juni 2024
Aktualisierte Funktionalität in Runtime Monitoring	Runtime Monitoring hat eine neue Security Agent-Version 1.2.0 für die Amazon EC2-Ressource veröffentlicht. Informationen zu Versionshinweisen finden Sie unter GuardDuty Security Agent für Amazon EC2-Instance. Informationen zur manuellen Aktualisierung des Security Agents auf diese Release-Version finden Sie unter Manuelles Verwalten des Security Agents für die Amazon EC2-Instance.	13. Juni 2024

Neue Funktion — Malware-Schutz für Verfügbarkeit in der S3-Region	GuardDuty Malware Protection for S3 ist jetzt in allen kommerziellen Regionen verfügbar, in denen GuardDuty es verfügbar ist. Mit dieser Funktion können Sie neu in Amazon S3-Buckets hochgeladene Objekte nach potenzieller Malware und verdächtigen Uploads durchsuchen und Maßnahmen ergreifen, um sie zu isolieren, bevor sie in nachgelagerte Prozesse aufgenommen werden. Informationen zur Aktivierung von Malware Protection for S3 finden Sie unter GuardDuty Malware Protection for S3.	12. Juni 2024

Neue Funktion — Malware-Schutz für S3	GuardDuty kündigt die allgemeine Verfügbarkeit von Malware Protection for S3 an, mit dem Sie neu in Amazon S3-Buckets hochgeladene Objekte nach potenzieller Malware und verdächtigen Uploads durchsuchen und Maßnahmen ergreifen können, um sie zu isolieren, bevor sie in nachgelagerte Prozesse aufgenommen werden. Diese Funktion wird vollständig von verwaltet. AWS GuardDuty veröffentlicht das Ergebnis des S3-Objektscans auf Ihrem EventBridge Standard-Event-Bus. Sie können zulassen GuardDuty , dass Ihren gescannten S3-Objekten Tags hinzugefügt werden. Sie können nachgelagerte Workflows erstellen, z. B. die Isolierung in einen Quarantäne-Bucket, oder Bucket-Richtlinien mithilfe von Tags definieren, die verhindern, dass Benutzer oder Anwendungen auf bestimmte Objekte zugreifen. Weitere Informationen finden Sie unter GuardDuty Malware-Schutz für S3. Derzeit ist es in den folgenden Regionen verfügbar: • USA Ost (Nord-Virginia)	11. Juni 2024

	• USA Ost (Ohio) • USA West (Oregon) • Europa (Irland) • Europa (Frankfurt) • Europa (Stockholm) • Asien-Pazifik (Sydney) • Asien-Pazifik (Tokio) • Asien-Pazifik (Singapur)	
AmazonGuardDutyFullAccess-Richtlinie aktualisiert	Es wurde eine Berechtigung hinzugefügt, die es Ihnen ermöglicht, eine IAM-Rolle zu übertragen, GuardDuty wenn Sie Malware Protection for S3 aktivieren. Weitere Informationen zu diesem Richtlinien-Update finden Sie unter AWS Verwaltete Richtlinie: AmazonGuardDutyFullAccess.	10. Juni 2024
Aktualisierte Funktionen in GuardDuty RDS Protection	RDS Protection erweitert die Unterstützung zur Überwachung der Anmeldeaktivitäten auf Ihren RDS for PostgreSQL-Datenbanken. Im Rahmen dieser Erweiterung beginnt GuardDuty automatisch die Überwachung der Anmeldedaten von RDS for PostgreSQL-Datenbanken für Konten, für die RDS Protection bereits aktiviert ist. GuardDuty Weitere Informationen finden Sie unter RDS-Schutz.	6. Juni 2024

Aktualisierte Funktionalität in GuardDuty Runtime Monitoring — Fargate (nur Amazon ECS)	Runtime Monitoring hat eine neue Agentenversion 1.2.0 für Ressourcen AWS Fargate (nur Amazon ECS) veröffentlicht. Weitere Informationen zu Versionshinweisen finden Sie unter GuardDuty Security Agent für Fargate-ECS.	31. Mai 2024
Aktualisierte Funktionalität in GuardDuty Malware Protection for EC2	Für jedes Amazon EBS-Volume, das an Ihre Amazon EC2-Instances und Container-Workloads angehängt ist, hat GuardDuty Malware Protection for EC2 die Größe des EBS-Volumes, das gescannt wird, auf bis zu 2048 GB erhöht. Informationen zum Scannen von Amazon EBS-Volumes, die an Ihre Instances angeschlossen sind, finden Sie unter Malware Protection for EC2. GuardDuty	29. Mai 2024
Die Funktionalität in Runtime Monitoring wurde aktualisiert	Runtime Monitoring für ECS-Fargate Amazon-Ressourcen unterstützt jetzt die Erkennung potenzieller Bedrohungen für Ihre Aufgaben, die von AWS Batch und gestartet wurden AWS CodePipeline. Weitere Informationen finden Sie unter So funktioniert Runtime Monitoring mit Fargate (nur Amazon ECS).	28. Mai 2024

Die Funktionalität in Runtime Monitoring wurde aktualisiert	Runtime Monitoring hat eine neue Agentenversion 1.6.1 für Amazon EKS-Ressourcen veröffentlicht. Informationen zu Versionshinweisen finden Sie im Versionsverlauf des EKS-Add-On-Agents.	14. Mai 2024
Erweiterte Regionsunterstützung für Runtime Monitoring	GuardDuty erweitert die Unterstützung für Runtime Monitoring auf die Region Kanada West (Calgary) . Informationen zu den ersten Schritten mit Runtime Monitoring finden Sie unter Runtime Monitoring https://docs.aws.amazon.com/guardduty/latest/ug/runtime-monitoring-configuration.html aktivieren.	7. Mai 2024

Erweiterte Regionsunterstützung für RDS Protection	GuardDuty erweitert die Unterstützung von RDS Protection auf Folgendes AWS-Regionen: • Kanada West (Calgary) • Asien-Pazifik (Hyderabad) • Europa (Spain) • Europa (Zürich) • Naher Osten (VAE) • Israel (Tel Aviv) • Asien-Pazifik (Melbourne) Informationen zur Aktivierung dieser Funktion finden Sie unter RDS-Schutz.	3. Mai 2024
Die Funktionalität in Runtime Monitoring wurde aktualisiert	Runtime Monitoring hat eine neue Agentenversion 1.1.0 für Ressourcen AWS Fargate (nur Amazon ECS) veröffentlicht. Weitere Informationen zu Versionshinweisen finden Sie unter GuardDuty Security Agent für Fargate-ECS.	1. Mai 2024
Die Funktionalität in Runtime Monitoring wurde aktualisiert	Runtime Monitoring hat eine neue Agentenversion 1.6.0 für Amazon EKS-Ressourcen veröffentlicht. Informationen zu Versionshinweisen finden Sie im Versionsverlauf des EKS-Add-On-Agents.	29. April 2024

Unterstützung für IPAddressv6	GuardDuty hat IPAddressV6-Unterstützung für lokale und Remote-IP-Details hinzugefügt. Sie können die zugehörigen Filterattribute verwenden, um GuardDuty Ergebnisse zu filtern oder Unterdrückungsregeln zu erstellen.	18. April 2024
Die Konsolenoberfläche wurde aktualisiert, um den Export von Ergebnissen zu konfigurieren	GuardDuty hat die Konsolenoberfläche aktualisiert, um die in Ihrem AWS-Konten generierten Ergebnisse in einen Amazon S3-Bucket zu exportieren. Weitere Informationen finden Sie unter GuardDuty Ergebnisse exportieren.	1. April 2024
Aktualisierte Funktionalität in Runtime Monitoring	Runtime Monitoring hat eine neue Security Agent-Version 1.1.0 für die Amazon EC2-Ressource veröffentlicht. Diese Version unterstützt die GuardDuty automatische Agentenkonfiguration in Runtime Monitoring für Amazon EC2-Instances. Informationen zu Versionshinweisen finden Sie unter GuardDuty Sicherheitsagent für Amazon EC2-Instance.	28. März 2024

Allgemeine Verfügbarkeit von Runtime Monitoring für Amazon EC2-Instances	GuardDuty kündigt die allgemeine Verfügbarkeit (GA) von Runtime Monitoring für Amazon EC2-Instances an. Jetzt haben Sie die Möglichkeit, die automatische Agentenkonfiguration zu aktivieren, die es ermöglicht, den Security Agent für Ihre Amazon EC2-Instances in Ihrem Namen GuardDuty zu installieren und zu verwalten. Mit dem GuardDuty automatisierten Agenten können Sie auch Inklusions- oder Ausschluss-Tags verwenden, um Sie darüber GuardDuty zu informieren, dass der Security Agent nur auf ausgewählten Amazon EC2-Instances installiert und verwaltet werden soll. Weitere Informationen finden Sie unter So funktioniert Laufzeit-Überwachung mit Amazon-EC2-Instances. Liste neuer Befundarten, die zusammen mit dieser GA veröffentlicht wurden • Execution:Runtime/SuspiciousTool • Execution:Runtime/SuspiciousCommand • DefenseEvasion:Runtime/SuspiciousCommand	28. März 2024

- DefenseEvasion:Runtime/PtraceAntiDebugging
- Execution:Runtime/MaliciousFileExecuted

Amazon GuardDuty hat die Service-linked Rolle (SLR) aktualisiert	Verwenden Sie AWS Systems Manager Aktionen, um SSM-Zuordnungen auf Amazon EC2-Instances zu verwalten, wenn Sie GuardDuty Runtime Monitoring mit automatisiertem Agenten für Amazon EC2 aktivieren. Wenn die GuardDuty automatische Agentenkonfiguration deaktiviert ist, werden nur die EC2-Instances GuardDuty berücksichtigt, die über ein Inklusions-Tag (:) verfügen. `GuardDutyManaged true` • Die folgende Liste zeigt die neuen Berechtigungen: `"ssm:DescribeAssociation", "ssm:DeleteAssociation", "ssm:UpdateAssociation", "ssm:CreateAssociation", "ssm:StartAssociationsOnce", "ssm:AddTagsToResource", "ssm:CreateAssociation", "ssm:UpdateAssociation", "ssm:SendCommand", "ssm:GetCommandInvocation"`	26. März 2024

Die Funktionalität in Runtime Monitoring wurde aktualisiert	Mit der neuesten Version v1.5.0 des GuardDuty Security Agents (Add-on) für Amazon EKS unterstützt zt Runtime Monitoring jetzt die Konfiguration bestimmte r Parameter Ihres GuardDuty Security Agents, wie CPU- und Speichereinstellun gen, `PriorityClass` Einstellungen und DNS-Richt linieneinstellungen. Weitere Informationen finden Sie unter Konfiguration der GuardDuty Security Agent-Parameter (EKS-Add-on).	7. März 2024
Die Funktionalität in Runtime Monitoring wurde aktualisiert	Runtime Monitoring hat eine neue Agentenversion 1.5.0 für Amazon EKS-Ressourcen veröffentlicht. Informationen zu Versionshinweisen finden Sie im Versionsverlauf des EKS-Add-On-Agents.	7. März 2024
Unterstützung für Canada West (Calgary)	Amazon GuardDuty ist jetzt in der Region Kanada West (Calgary) verfügbar. Einige der darin enthaltenen Schutzplä ne sind in dieser Region GuardDuty möglicherweise nicht verfügbar. Die neuesten Informationen finden Sie unter Regionen und Endpunkte.	6. März 2024

Die Funktionalität in Runtime Monitoring wurde aktualisiert	Die GuardDuty Security Agent-Versionen 1.0.0 und 1.1.0 für Amazon EKS-Cluster werden ab dem 14. Mai 2024 nicht mehr unterstützt. Informationen darüber, welche Schritte Sie vor dem Ende des Standardsupports unternehmen können, finden Sie unter GuardDuty Security Agent für Amazon EKS-Cluster.	16. Februar 2024
Die Funktionalität in Runtime Monitoring wurde aktualisiert	Runtime Monitoring unterstützt die neueste Kubernetes-Version 1.29 mit der vorhandenen Security Agent-Version 1.4.1. Der Support ist seit dem Start dieser Kubernetes-Version verfügbar. Informationen zu den unterstützten Kubernetes-Versionen finden Sie unter Vom Security Agent unterstützte Kubernetes-Versionen. GuardDuty	16. Februar 2024

Aktualisierte Funktionalität in Runtime Monitoring — Regionale Verfügbarkeit	GuardDuty Runtime Monitoring unterstützt jetzt die gemeinsame Nutzung von Amazon VPC innerhalb derselben AWS Organizations. GuardDuty Die Service-Linked Role (SLR) hat eine neue Berechtigung — `organizations:DescribeOrganization` sie hilft beim Abrufen der Organisations-ID für das gemeinsam genutzte Amazon VPC-Konto, um die Endpunktrichtlinie festzulegen. Informationen zu den Voraussetzungen für die Verwendung eines gemeinsam genutzten Amazon VPC-Endpunkts in Runtime Monitoring finden Sie unter Support für gemeinsam genutzte Amazon VPC. Diese Funktion ist in allen Regionen verfügbar, in denen Runtime Monitoring GuardDuty unterstützt wird.	12. Februar 2024

Aktualisierte Funktionalität in Runtime Monitoring — Regionale Verfügbarkeit	GuardDuty Runtime Monitoring unterstützt jetzt die gemeinsame Nutzung von Amazon VPC innerhalb derselben AWS Organizations. GuardDuty Die Service-Linked Role (SLR) hat eine neue Berechtigung — `organizations:DescribeOrganization` sie hilft beim Abrufen der Organisations-ID für das gemeinsam genutzte Amazon VPC-Konto, um die Endpunktrichtlinie festzulegen. Informationen zu den Voraussetzungen für die Verwendung eines gemeinsam genutzten Amazon VPC-Endpunkts in Runtime Monitoring finden Sie unter Support für gemeinsam genutzte Amazon VPC. Derzeit ist diese Funktion in einigen der verfügbar . AWS-Regionen Weitere Informationen finden Sie unter -Regionen und Endpunkte.	9. Februar 2024
Aktualisierte Funktionalität mit Unterstützung für das neue AWS-Regionen Programm — Malware Protection for EC2	Malware Protection for EC2 unterstützt jetzt das Scannen der EBS-Volumes, mit denen Von AWS verwaltete Schlüssel in der Region USA West (Oregon) verschlüsselt wurde.	6. Februar 2024

Aktualisierte Funktionalität mit Unterstützung für das neue Programm Malware AWS-Regionen Protection for EC2	Malware Protection for EC2 unterstützt jetzt das Scannen der EBS-Volumes, die mit Von AWS verwaltete Schlüssel folgenden Daten verschlüsselt sind: AWS-Regionen • Asien-Pazifik (Singapur) (`ap-southeast-1`) • Europa (Frankfurt) (`eu-central-1`) • Asien-Pazifik (Osaka) (`ap-northeast-3`) • USA Ost (Ohio) (`us-east-2`) • Europa (Mailand) (`eu-south-1`) • Asien-Pazifik (Tokio) (`ap-northeast-1`) • Asien-Pazifik (Seoul) (`ap-northeast-2`) • Kanada (Zentral) (`ca-central-1`) • Europa (Irland) (`eu-west-1`) • USA Ost (Nord-Virginia) (`us-east-1`)	5. Februar 2024

Aktualisierte Funktionalität in Runtime Monitoring	GuardDuty Runtime Monitoring hat eine neue GuardDuty Security Agent-Version (v1.0.2) für Amazon EC2-Instances veröffentlicht. Diese Agentenversion beinhaltet Unterstützung für die neuesten Amazon ECS-AMIs. Weitere Informationen zum Veröffentlichungsverlauf von Agenten finden Sie unter GuardDuty Security Agent für Amazon EC2-Instances.	2. Februar 2024

Aktualisierte Funktionalität mit Unterstützung für das neue Programm AWS-Regionen Malware Protection for EC2	Malware Protection for EC2 unterstützt jetzt das Scannen der Amazon EBS-Volumes, die mit Von AWS verwaltete Schlüssel folgenden Daten verschlüsselt sind: AWS-Regionen • Europa (London) (`eu-west-2`) • Europa (Stockholm) (`eu-north-1`) • Asien-Pazifik (Hongkong) (`ap-east-1`) • Afrika (Kapstadt) (`af-south-1`) • Naher Osten (Bahrain) (`me-south-1`) • Asien-Pazifik (Hyderabad) (`ap-south-2`) • Europa (Spanien) (`eu-south-2`) • Asien-Pazifik (Melbourne) (`ap-southeast-4`) • Asien-Pazifik (Sydney) (`ap-southeast-2`) • Israel (Tel Aviv) (`il-central-1`)	31. Januar 2024

Die Verwaltung von Konten wurde aktualisiert mit AWS Organizations	Der Inhalt unter Konten verwalten mit AWS Organizations wurde neu organisiert. , Schritte zur Änderung des delegierten GuardDuty Administratorkontos hinzugefügt und Grundlegendes zur Beziehung zwischen GuardDuty Administratorkonto und Mitgliedskonten aktualisiert.	30. Januar 2024
Aktualisierte Funktionalität mit Unterstützung für neue AWS-Regionen	Malware Protection for EC2 unterstützt jetzt das Scannen der EBS-Volumes, die wie folgt Von AWS verwaltete Schlüssel verschlüsselt sind: AWS-Regionen • Asien-Pazifik (Jakarta) (`ap-southeast-3`) • USA West (Nordkalifornien) (`us-west-1`) • Naher Osten (VAE) (`me-central-1`) • Europa (Zürich) (`eu-central-2`) • Asien-Pazifik (Mumbai) (`ap-south-1`) • Südamerika (São Paulo) (`sa-east-1`)	29. Januar 2024

Aktualisierte Funktionalität in Malware Protection for EC2	Malware Protection for EC2 unterstützt jetzt das Scannen der mit verschlüsselten EBS-Volumes. Von AWS verwaltete SchlüsselMalware Protection for EC2 Service Linked Role (SLR) hat zwei neue Berechtigungen — und. `GetSnapshotBlock` `ListSnapshotBlocks` Diese Berechtigungen helfen dabei, den Snapshot eines EBS-Volumes (verschlüsselt mit Von AWS verwalteter Schlüssel) von Ihrem GuardDuty abzurufen AWS-Konto und auf das GuardDuty Dienstkonto zu kopieren, bevor Sie den Malware-Scan starten. Derzeit ist diese Funktion nur in Europa (Paris) (`eu-west-3`) verfügbar. Weitere Informationen finden Sie unter Unterstützte Volumes für die Malware-Suche.	25. Januar 2024

Die Funktionalität in Runtime Monitoring wurde aktualisiert	GuardDuty Runtime Monitoring hat eine neue GuardDuty Security Agent-Version (v1.0.1) mit allgemeiner Leistungsoptimierung und Verbesserungen veröffentlicht. Weitere Informationen zum Veröffentlichungsverlauf der Agenten finden Sie unter GuardDuty Security Agent für Amazon EC2-Instances.	23. Januar 2024
Die Funktionalität in Runtime Monitoring wurde aktualisiert	Runtime Monitoring hat eine neue Agentenversion 1.4.1 für Amazon EKS-Ressourcen veröffentlicht. Weitere Informationen finden Sie in der Versionshistorie des EKS-Add-On-Agenten.	16. Januar 2024
Runtime Monitoring hat den neuen Agenten v1.4.0 für Amazon EKS-Ressourcen veröffentlicht	Runtime Monitoring hat eine neue Agentenversion 1.4.0 für Amazon EKS-Ressourcen veröffentlicht. Weitere Informationen finden Sie in der Versionshistorie des EKS-Add-On-Agenten.	21. Dezember 2023

Die Ergebnisarten Europa (Zürich), Europa (Spanien), Asien-Pazifik (Hyderabad), Asien-Pazifik (Melbourne) und Israel (Tel Aviv) wurden um S3 und AWS CloudTrail maschinelles Lernen (ML) erweitert	Das folgende S3 und die CloudTrail Ergebnisse, die das anomale Verhalten mithilfe GuardDuty des Modells für maschinelles Lernen (ML) zur Erkennung von Anomalien identifizieren, sind jetzt in den Regionen Europa (Zürich), Europa (Spanien), Asien-Pazifik (Hyderabad), Asien-Pazifik (Melbourne) und Israel (Tel Aviv) verfügbar: • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior • Exfiltration:IAMUser/AnomalousBehavior • Impact:IAMUser/AnomalousBehavior • CredentialAccess:IAMUser/AnomalousBehavior • DefenseEvasion:IAMUser/AnomalousBehavior • InitialAccess:IAMUser/AnomalousBehavior	21. Dezember 2023

	• Persistence:IAMUser/AnomalousBehavior • PrivilegeEscalation:IAMUser/AnomalousBehavior • Discovery:IAMUser/AnomalousBehavior	
GuardDuty unterstützt 50.000 Mitgliedskonten über AWS Organizations	Ein delegierter GuardDuty Administrator kann jetzt maximal 50.000 Mitglieds konten über AWS Organizat ions verwalten. Dazu gehören auch maximal 5000 Mitglieds konten, die dem GuardDuty Administratorkonto auf Einladung zugeordnet wurden.	20. Dezember 2023
GuardDuty Die Unterstützung für Runtime Monitoring wurde auf 19 erweitert AWS-Regio nen	Runtime Monitoring ist jetzt in den Regionen Asien-Paz ifik (Jakarta), Europa (Paris), Asien-Pazifik (Osaka), Asien-Pazifik (Seoul), Naher Osten (Bahrain), Europa (Spanien) , Asien-Pazifik (Hyderaba d), Asien-Pazifik (Melbourn e), Israel (Tel Aviv), USA West (Nordkalifornien), Europa (London), Asien-Pazifik (Hongkong), Europa (Mailand), Naher Osten (VAE), Südamerika (São Paulo) verfügbar), Asien-Pazifik (Mumbai), Kanada (Zentral) , Afrika (Kapstadt), Europa (Zürich).	6. Dezember 2023

GuardDuty erweitert die Runtime Monitoring-Funktion	GuardDuty Kündigt zusätzlich zur Erkennung von Bedrohungen für Ihre Amazon EKS-Cluster die allgemeine Verfügbarkeit von Runtime Monitoring an, um Bedrohungen für Ihre Amazon ECS-Workloads zu erkennen, sowie eine Vorabversion zur Erkennung von Bedrohungen für Ihre Amazon EC2-Instances. Weitere Informationen darüber, welche Geräte AWS-Regionen derzeit Runtime Monitoring unterstützen, finden Sie unter Regionen und Endpunkte.	26. November 2023

Amazon GuardDuty hat die Service-linked Rolle (SLR) aktualisiert	GuardDuty hat neue Berechtigungen hinzugefügt, um Amazon ECS-Aktionen zum Verwalten und Abrufen von Informationen über die Amazon ECS-Cluster zu verwenden und die Amazon ECS-Kontoeinstellungen mit `guarddutyActivate` zu verwalten. Die Aktionen, die Amazon ECS betreffen, rufen auch die Informationen über die zugehörigen Tags ab. GuardDuty • Die folgenden Berechtigungen wurden im Rahmen der GuardDuty Erweiterung der Runtime Monitoring-Funktion hinzugefügt: `"ecs:ListClusters", "ecs:DescribeClusters", "ecs:PutAccountSettingDefault"`	26. November 2023
Die AWS verwalteten Richtlinien wurden aktualisiert	GuardDuty hat der AWS verwalteten Richtlinie eine neue Berechtigung hinzugefügt: AmazonGuardDutyFullAccess und AmazonGuardDutyReadOnlyAccess. `organizations:ListAccounts`	16. November 2023

GuardDuty hat neue Suchtypen veröffentlicht, die EKS Audit Log Monitoring verwenden.	EKS Audit Log Monitoring unterstützt jetzt die folgenden Suchtypen im asiatisch-pazifischen Raum (Melbourne) (`ap-southeast-4`). • CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated • Execution:Kubernetes/AnomalousBehavior.ExecInPod • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount • Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated • Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	11. November 2023

GuardDuty hat neue Erkennungstypen veröffentlicht, die EKS Audit Log Monitoring verwenden.	EKS Audit Log Monitoring unterstützt jetzt die folgenden Ergebnisarten in den Regionen Asien-Pazifik (Hyderabad`ap-south-2`) (), Europa (Zürich`eu-central-2`) () und Europa (Spanien) (`eu-south-2`). • CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated • Execution:Kubernetes/AnomalousBehavior.ExecInPod • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount • Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	10. November 2023

- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

GuardDuty hat neue Erkennungstypen veröffentlicht, die EKS Audit Log Monitoring verwenden.	EKS Audit Log Monitoring unterstützt jetzt die folgenden Suchtypen. Diese Ergebnisarten sind in den Regionen Asien-Pazifik (Hyderabad) (`ap-south-2`), Europa (Zürich) (`eu-central-2`), Europa (Spanien) (`eu-south-2`) und Asien-Pazifik (Melbourne) (`ap-southeast-4`) noch nicht verfügbar. • CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated • Execution:Kubernetes/AnomalousBehavior.ExecInPod • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount • Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	8. November 2023

	• PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated • Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	
EKS-Laufzeit-Überwachung hat den neuen Agenten v1.3.1 veröffentlicht	EKS Runtime Monitoring hat eine neue Agentenversion 1.3.1 veröffentlicht, die wichtige Sicherheitspatches und Updates enthält.	23. Oktober 2023
Neues Filterattribut für die Erkenntnis	GuardDuty hat ein neues Kriterium hinzugefügt, um die generierten Ergebnisse zu filtern. Das Domänensuffix für DNS-Anfragen gibt die Domain der zweiten und obersten Ebene an, die an der Aktivität beteiligt ist, die GuardDuty zur Generierung des Ergebnisses geführt hat.	17. Oktober 2023
EKS-Laufzeit-Überwachung hat den neuen Agenten v1.3.0 veröffentlicht, der Kubernetes Version 1.28 unterstützt	EKS Runtime Monitoring hat eine neue Agentenversion 1.3.0 veröffentlicht, die Kubernetes-Version 1.28 unterstützt. Unterstützung für Ubuntu hinzugefügt. Weitere Informationen finden Sie in der Versionshistorie des EKS-Add-On-Agenten.	05. Oktober 2023

Für die Regionen Asien-Pazifik (Jakarta) und Naher Osten (VAE) wurden die auf S3 und AWS CloudTrail maschinellem Lernen (ML) basierenden Ergebnistypen hinzugefügt	Das folgende S3 und die CloudTrail Ergebnisse, die das anomale Verhalten mithilfe GuardDuty des Modells für maschinelles Lernen (ML) zur Erkennung von Anomalien identifizieren, sind jetzt in den Regionen Asien-Pazifik (Jakarta) und Naher Osten (VAE) verfügbar: • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior • Exfiltration:IAMUser/AnomalousBehavior • Impact:IAMUser/AnomalousBehavior • CredentialAccess:IAMUser/AnomalousBehavior • DefenseEvasion:IAMUser/AnomalousBehavior • InitialAccess:IAMUser/AnomalousBehavior • Persistence:IAMUser/AnomalousBehavior	20. September 2023

	• PrivilegeEscalation:IAMUser/AnomalousBehavior • Discovery:IAMUser/AnomalousBehavior	
GuardDuty EKS Runtime Monitoring führt die Verwaltung eines GuardDuty Sicherheitsagenten auf Clusterebene ein	EKS Runtime Monitoring bietet Unterstützung für die Verwaltung des GuardDuty Security Agents für einzelne EKS-Cluster, um die Laufzeitereignisse nur von diesen ausgewählten Clustern aus zu überwachen. EKS-Laufzeit-Überwachung erweitert diese Funktion um die Unterstützung von Tags.	13. September 2023
GuardDuty Malware Protection for EC2 erweitert die Unterstützung auf weitere AWS-Regionen	Malware Protection for EC2 ist jetzt im asiatisch-pazifischen Raum (Hyderabad), im asiatisch-pazifischen Raum (Melbourne), in Europa (Zürich) und in Europa (Spanien) verfügbar.	11. September 2023

GuardDuty ist jetzt in der Region Israel (Tel Aviv) verfügbar	Die Region Israel (Tel Aviv) wurde zur Liste der Orte hinzugefügt AWS-Regionen , an denen sie jetzt verfügbar GuardDuty ist. Die folgenden Schutzpläne sind auch in der Region Israel (Tel Aviv) verfügbar: • EKS-Schutz umfasst EKS Audit Log Monitoring EKS-Laufzeit-Überwachung. • Lambda Protection. • Malware-Schutz für EC2. • S3-Schutz. Weitere Informationen zur Verfügbarkeit von Schutzplänen in der Region Israel (Tel Aviv) finden Sie unter Regionen und Endpunkte.	24. August 2023
GuardDuty Konfiguration zur automatischen Aktivierung für Ihr Unternehmen auf Schutzplanebene hinzugefügt	Aktualisieren Sie die Organisationskonfiguration für die Schutzpläne in Ihrer Region. Mögliche Konfigurationsoptionen sind entweder „für alle Konten aktivieren“, „für neue Konten automatisch aktivieren“ oder „für kein Konto in Ihrer Organisation automatisch aktivieren“.	16. August 2023

S3-Erkennungstypen, die mithilfe GuardDuty des ML-Modells (Anomaly Detection Machine Learning) anomales Verhalten identifizieren, sind jetzt in der Region Asien-Pazifik (Osaka) verfügbar	Die folgenden Erkenntnistypen sind jetzt in der Region Asien-Pazifik (Osaka) verfügbar: • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior	10. August 2023
EKS-Laufzeit-Überwachung ist jetzt in Asien-Pazifik (Melbourne) verfügbar	EKS Runtime Monitoring innerhalb von GuardDuty EKS Protection ermöglicht die Runtime-Erkennung von Bedrohungen für Ihre Amazon EKS-Cluster in der Umgebung. AWS Die Funktion wird jetzt in der Region Asien-Pazifik (Melbourne) unterstützt.	08. August 2023
Die Liste der GuardDuty Ergebnisse, die den GuardDuty-initiated Malware-Scan aufrufen, wurde aktualisiert	Bestimmte Erkennungstypen von EKS Runtime Monitoring können jetzt einen GuardDuty -initiated Malware-Scan in Ihrem starten. AWS-Konto	19. Juli 2023

GuardDuty unterstützt 10.000 Mitgliedskonten über AWS Organizations	Ein GuardDuty Administratorkonto kann jetzt maximal 10.000 Mitgliedskonten über verwalten AWS Organizations. Dazu gehören auch maximal 5000 Mitgliedskonten, die dem GuardDuty Administratorkonto auf Einladung zugeordnet wurden.	29. Juni 2023
EKS-Laufzeit-Überwachung kündigt drei neue Erkenntnistypen an.	EKS-Laufzeit-Überwachung unterstützt drei neue Erkenntnistypen, die auf der Prozessinjektions-Methode basieren. Die neuen Ergebnistypen sind DefenseEvasion:Runtime/ProcessInjection.Proc DefenseEvasion:Runtime/ProcessInjection.Ptrace, und DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite.	22. Juni 2023
EKS-Laufzeit-Überwachung hat den neuen Agenten v1.2.0 veröffentlicht, der Kubernetes Version 1.27 unterstützt	EKS Runtime Monitoring hat eine neue Agentenversion 1.2.0 veröffentlicht, die auch ARM64-based Instanzen unterstützt. Unterstützung für Bottlerocket hinzugefügt. Weitere Informationen finden Sie in der Versionshistorie des EKS-Add-On-Agenten.	16. Juni 2023

GuardDuty Die Konsole bietet eine zusammenfassende Ansicht Ihrer Ergebnisse.	Das Übersichts-Dashboard in der GuardDuty Konsole bietet eine aggregierte Ansicht der GuardDuty Ergebnisse. Derzeit zeigt das Dashboard mithilfe verschiedener Widgets Daten für die letzten 10.000 Ergebnisse an, die für Ihr Konto (oder Mitgliedskonten, wenn Sie ein GuardDuty Administratorkonto sind) für die aktuelle Region generiert wurden.	12. Juni 2023
EKS Audit Log Monitoring ist jetzt in Asien-Pazifik (Hyderabad), Asien-Pazifik (Melbourne), Europa (Zürich) und Europa (Spanien) verfügbar	Aktivieren Sie EKS Audit Log Monitoring (in EKS Protection) für Ihre Konten, um die EKS-Auditprotokolle aus Ihren Amazon EKS-Clustern zu überwachen und sie auf potenziell bösartige und verdächtige Aktivitäten zu analysieren.	01. Juni 2023
EKS Audit Log Monitoring ist jetzt in Naher Osten (VAE) verfügbar	EKS Audit Log Monitoring ist jetzt im Nahen Osten (VAE) verfügbar. Aktivieren Sie EKS Audit Log Monitoring für Ihre Konten, um EKS-Auditprotokolle aus Ihren Amazon EKS-Clustern zu überwachen und sie auf potenziell bösartige und verdächtige Aktivitäten zu analysieren.	3. Mai 2023

GuardDuty Malware Protection for EC2 kündigt einen On-demand Malware-Scan an	Malware Protection for EC2 hilft Ihnen dabei, das potenzielle Vorhandensein von Malware in den Amazon EBS-Volumes zu erkennen, die an Ihre Amazon EC2-Instances und Container-Workloads angehängt sind. Es bietet jetzt zwei Arten von Scans — GuardDuty initiierte und On-Demand-Scans. GuardDuty -initiated Der Malware-Scan initiiert nur dann automatisch einen Scan ohne Agenten in den Amazon EBS-Volumes, wenn eines der Ergebnisse GuardDuty generiert wird, die den Malware-Scan auslösen. GuardDuty-initiated Sie können einen On-demand Malware-Scan für Amazon EC2-Instances in Ihrem Konto einleiten, indem Sie den Amazon-Ressourcennamen (ARN) angeben, der dieser Amazon EC2-Instance zugeordnet ist. Weitere Informationen darüber, wie sich beide Scantypen unterscheiden, finden Sie unter Malware-Schutz für EC2. • GuardDuty-initiated Malware-Scan • On-demand Malware-Scan	27. April 2023

GuardDuty kündigt Lambda Protection an	Lambda Protection hilft Ihnen, potenzielle Sicherheitsbedrohungen in Ihren AWS Lambda -Funktionen zu erkennen. • Lambda-Protection-Erkenntnistypen • Behebung einer potenziell gefährdeten Lambda-Funktion	20. April 2023
GuardDuty ist jetzt in der Region Asien-Pazifik (Melbourne) verfügbar	Asien-Pazifik (Melbourne) zur Liste der verfügbaren AWS-Regionen GuardDuty Orte hinzugefügt. Informationen darüber, welche Funktionen in dieser Region verfügbar sind, finden Sie unter Regionen und Endpunkte.	19. April 2023
GuardDuty 3 neue Typen von EC2-Ergebnissen hinzugefügt	GuardDuty führt neue Suchtypen ein, um die Verwendung externer DNS-Resolver und verschlüsselter DNS-Technologien zu erkennen. Informationen darüber AWS-Regionen , wo diese Suchtypen unterstützt werden, finden Sie unter Regionen und Endpunkte. • DefenseEvasion:EC2/UnusualDNSResolver • DefenseEvasion:EC2/UnusualDoHActivity • DefenseEvasion:EC2/UnusualDoTActivity	5. April 2023

GuardDuty kündigt EKS-Laufzeitüberwachung in EKS Protection an	EKS Runtime Monitoring in EKS Protection bietet zur Laufzeit die Erkennung von Bedrohungen für Ihre Amazon EKS-Cluster in der AWS Umgebung. Die Funktion verwendet einen Amazon-EKS-Add-On-Agenten (`aws-guardduty-agent`), der Laufzeit-Ereignisse aus Ihren EKS-Workloads sammelt. Nach GuardDuty Erhalt dieser Laufzeitereignisse werden sie überwacht und analysiert, um potenzielle verdächtige Sicherheitsbedrohungen zu identifizieren. Weitere Informationen finden Sie unter Erkenntnisdetails und Erkenntnistypen der EKS-Laufzeit-Überwachung.	30. März 2023

GuardDuty fügt eine neue Funktionalität hinzu — `autoEnableOrganizationMembers`	Amazon GuardDuty fügt eine neue Option zur Organisationskonfiguration hinzu, mit der GuardDuty Administratorkonten die für `ALL` die Mitglieder ihrer Organisation aktivierten GuardDuty Funktionen überprüfen und (falls erforderlich) durchsetzen können. Die beste Vorgehensweise besteht jetzt darin, `autoEnableOrganizationMembers` anstelle von `autoEnable` zu verwenden. `autoEnable` ist veraltet, wird aber immer noch unterstützt. Die folgenden APIs sind von dieser neuen Funktionalität betroffen: • DescribeOrganizationConfiguration • UpdateOrganizationConfiguration • DisassociateMembers • DeleteMembers • DisassociateFromAdministratorAccount • StopMonitoringMembers	23. März 2023

Die RDS-Schutzfunktion in Amazon GuardDuty ist jetzt allgemein verfügbar	GuardDuty RDS Protection überwacht und profiliert die RDS-Anmeldeaktivitäten, um verdächtiges Anmeldeverhalten auf Ihren Amazon Aurora-Datenbank-Instances zu identifizieren. Weitere Informationen dazu, welche AWS-Regionen unterstützen, finden Sie unter Regionen und Endpunkte.	16. März 2023

GuardDuty kündigt die Aktivierung der Funktion an	In der Vergangenheit ermöglichte die GuardDuty API die Konfiguration sowohl von Funktionen als auch von Datenquellen, aber jetzt werden alle neuen GuardDuty Schutztypen als Funktione n und nicht als Datenquel len konfiguriert. GuardDuty unterstützt die Datenquellen immer noch über die API, fügt aber keine neue API hinzu. Die Aktivierung von Funktionen wirkt sich auf das Verhalten der APIs aus, die zur Aktivierung verwendet werden, GuardDuty oder auf den darin enthaltenen Schutztyp GuardDuty. Wenn Sie Ihre GuardDuty Konten über eine API, ein SDK oder eine CFN-Vorlage verwalten , finden Sie weitere Informati onen zu den GuardDuty API-Änderungen im März 2023.	16. März 2023
GuardDuty Malware Protection for EC2 ist jetzt in der Region Naher Osten (VAE) verfügbar	Die Funktion „Malware-Schutz für EC2“ in GuardDuty wird in der Region Naher Osten (VAE) unterstützt. Weitere Informationen finden Sie unter -Regionen und Endpunkte.	13. März 2023

Amazon GuardDuty hat die Service-linked Rolle (SLR) aktualisiert	GuardDuty hat die folgenden neuen Berechtigungen hinzugefügt, um die kommende GuardDuty EKS-Runtime Monitoring-Funktion zu unterstützen. • Verwenden Sie Amazon-EKS-Aktionen, um Informationen über die EKS-Cluster zu verwalten und abzurufen und EKS-Add-Ons auf EKS-Clustern zu verwalten . Die EKS-Aktionen rufen auch die Informationen zu den zugehörigen Tags ab GuardDuty. `"eks:ListClusters", "eks:DescribeCluster", "ec2:DescribeVpcEndpointServices", "ec2:DescribeSecurityGroups"`	08. März 2023
Amazon GuardDuty hat die Service-linked Rolle (SLR) aktualisiert	Die GuardDuty SLR wurde aktualisiert, um die Erstellung von Malware Protection for EC2 SLR zu ermöglichen, nachdem der Malware-Schutz für EC2 aktiviert wurde.	21. Februar 2023

GuardDuty erfordert TLS v1.2 oder höher	Für die Kommunikation mit AWS Ressourcen GuardDuty benötigt und unterstützt TLS v1.2 oder höher. Weitere Informationen finden Sie unter Datenschutz und Infrastruktursicherheit.	14. Februar 2023
GuardDuty ist jetzt in der Region Asien-Pazifik (Hyderabad) verfügbar	Die Region Asien-Pazifik (Hyderabad) wurde zur Liste der verfügbaren Standorte AWS-Regionen hinzugefügt GuardDuty . Weitere Informationen finden Sie unter -Regionen und Endpunkte.	14. Februar 2023
Das GuardDuty Amazon-Benutzerhandbuch entspricht den bewährten IAM-Praktiken	Aktualisierung des Leitfadens zur Ausrichtung an bewährten IAM-Methoden. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden in IAM.	10. Februar 2023
GuardDuty ist jetzt in der Region Europa (Spanien) verfügbar	Europa (Spanien) zur Liste der AWS-Regionen verfügbaren GuardDuty Standorte hinzugefügt. Weitere Informationen finden Sie unter - Regionen und Endpunkte.	8. Februar 2023
GuardDuty ist jetzt in der Region Europa (Zürich) verfügbar	Europa (Zurich) zur Liste der AWS-Regionen verfügbaren GuardDuty Standorte hinzugefügt. Weitere Informationen finden Sie unter - Regionen und Endpunkte.	12. Dezember 2022

Vorabversion einer neuen Funktion — GuardDuty RDS Protection	GuardDuty RDS Protection überwacht und profiliert die RDS-Anmeldeaktivitäten, um verdächtiges Anmeldeverhalten auf Ihren Amazon Aurora-Datenbank-Instances zu identifizieren. Derzeit ist es als Vorabversion in fünf AWS-Regionen verfügbar. Weitere Informationen finden Sie unter -Regionen und Endpunkte.	30. November 2022
GuardDuty ist jetzt in der Region Naher Osten (VAE) verfügbar	Naher Osten (VAE) zur Liste der AWS-Regionen verfügbaren GuardDuty Gebiete hinzugefügt. Weitere Informationen finden Sie unter -Regionen und Endpunkte.	6. Oktober 2022

Inhalt für eine neue Funktion hinzugefügt — GuardDuty Malware Protection for EC2	GuardDuty Der Malware-Schutz für EC2 ist eine optionale Erweiterung von Amazon. GuardDuty Malware Protection for EC2 GuardDuty identifiziert zwar die gefährdeten Ressourcen, erkennt aber auch die Malware, die die Ursache der Gefährdung sein könnte. Wenn Malware Protection for EC2 aktiviert ist, initiiert Malware Protection for EC2 jedes Mal, wenn verdächtiges Verhalten auf einer Amazon EC2-Instance oder einem Container-Workload GuardDuty erkannt wird, das auf Malware hindeutet, einen agentenlosen Scan auf den EBS-Volumes, die an die betroffenen EC2-Instance- oder Container-Workloads angeschlossen sind, um das Vorhandensein von GuardDuty Malware zu erkennen. Informationen zur Funktionsweise von Malware Protection for EC2 und zur Konfiguration dieser Funktion finden Sie unter Malware Protection for EC2. GuardDuty • Informationen zu den Ergebnissen von Malware	26. Juli 2022

	Protection for EC2 finden Sie unter Finding details. • Informationen zur Behebung der kompromittierten EC2-Instance und eines eigenständigen Containers finden Sie unter Behebung von Sicherheitsproblemen, die von entdeckt wurden. GuardDuty • Informationen zu den CloudWatch Überwachu ngsprotokollen für Malware-Scans und zu Gründen für das Überspringen einer Ressource während des Malware-Scans finden Sie unter Grundlegendes CloudWatch zu Protokollen und Übersprunggründen. • Informationen zu falsch positiven Bedrohung serkennungen finden Sie unter Melden von Fehlalarm en in GuardDuty Malware Protection for EC2.	
Ein Erkenntnistyp wurde außer Betrieb genommen	Exfiltration:S3/ObjectRead. Unusual wurde außer Betrieb genommen.	5. Juli 2022

Es wurden neue S3-Erkennungstypen hinzugefügt, die anomales Verhalten mithilfe GuardDuty des maschinellen Lernmodells (ML) zur Erkennung von Anomalien identifizieren.	Die folgenden neuen S3-Erkenntnistypen wurden hinzugefügt. Diese Erkenntnistypen identifizieren, ob eine API-Anfrage eine IAM-Entität auf ungewöhnliche Weise aufgerufen hat. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Taktiken von Angreifern in Verbindung gebracht werden. Weitere Informationen zu den einzelnen neuen Erkenntnissen finden Sie unter S3-Erkenntnistypen. • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior	5. Juli 2022

GuardDuty EKS-Protection-Inhalt hinzugefügt für GuardDuty	GuardDuty kann jetzt mithilfe der Überwachung der EKS-Auditprotokolle Ergebnisse für Ihre Amazon EKS-Ressourcen generieren. Informationen zur Konfiguration dieser Funktion finden Sie unter EKS-Schutz bei Amazon GuardDuty. Eine Liste der Ergebnisse, die für Amazon EKS-Ressourcen generiert werden GuardDuty können, finden Sie unter Kubernetes-Ergebnisse. Es wurden neue Anleitungen zur Behebung hinzugefügt, um die Behebung dieser Erkenntnisse zu unterstützen im Leitfaden zur Behebung von Erkenntnissen in Kubernetes.	25 Januar 2022
Es wurde eine neue Erkenntnis hinzugefügt	Die neue Erkenntnis UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS wurde hinzugefügt. Dieses Ergebnis informiert Sie, wenn ein AWS Konto außerhalb Ihrer Umgebung auf Ihre Instance-Anmeldeinformationen zugreift. AWS	20. Januar 2022

Die Erkenntnistypen wurden aktualisiert, um Probleme im Zusammenhang mit log4j leichter identifizieren zu können	Amazon GuardDuty hat die folgenden Erkennungstypen aktualisiert, um Probleme im Zusammenhang mit und zu identifizieren CVE-2021-44228 und zu priorisieren CVE-2021-45046:Backdoor:EC2/C&CActivity.B;Backdoor:EC2/C&CActivity.B!DNS;. Behavior:EC2/NetworkPortUnusual	22. Dezember 2021
Erkenntnis-Änderungen	UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration wurde geändert zu UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS. Diese verbesserte Version der Erkenntnisse erfasst die typischen Standorte, von denen aus Ihre Anmeldeinformationen verwendet werden, und reduziert so die Anzahl der Erkenntnisse aus dem Datenverkehr, der über lokale Netzwerke geleitet wird. UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	7. September 2021
Auf SLR aktualisieren GuardDuty	Die GuardDuty Spiegelre flexkamera wurde mit neuen Aktionen aktualisiert, um die Suchgenauigkeit zu verbessern.	3. August 2021

Es wurden Datenquelleninformationen für jeden Erkenntnistyp hinzugefügt.	Die Befundbeschreibungen enthalten jetzt Informationen über Datenquellen, die zur Generierung des Ergebnisses GuardDuty verwendet wurden.	10. Mai 2021
13 Erkenntnistypen entfernt.	13 Ergebnisse wurden entfernt und durch neue Anomalous Behavoir Ergebnisse ersetzt. Persistence:IAMUser/NetworkPermissions, Persistence:IAMUser/ResourcePermissions, Persistence:IAMUser/UserPermissions Privilege Escalation:IAMUser/AdministrativePermissions, Recon:IAMUser/NetworkPermissions, Recon:IAMUser/ResourcePermissions, Recon:IAMUser/UserPermissions, ResourceConsumption:IAMUser/ComputeResources, Stealth:IAMUser/LoggingConfiguration Modified, Discovery:S3/BucketEnumeration.Unusual Impact:S3/ObjectDelete.Unusual, Impact:S3/PermissionsModification.Unusual, und UnauthorizedAccess:IAMUser/ConsoleLogin.	12. März 2021

Es wurden 8 neue Erkenntnistypen für anomales Verhalten hinzugefügt.	Es wurden 8 neue IAMUser-Erkenntnistypen hinzugefügt, die auf anomalem Verhalten für IAM-Prinzipale basieren. CredentialAccess:IAMUser/AnomalousBehavior, DefenseEvasion:IAMUser/AnomalousBehavior, Discovery:IAMUser/AnomalousBehavior, Exfiltration:IAMUser/AnomalousBehavior, Impact:IAMUser/AnomalousBehavior, InitialAccess:IAMUser/AnomalousBehavior, Persistence:IAMUser/AnomalousBehavior, PrivilegeEscalation:IAMUser/AnomalousBehavior.	12. März 2021
EC2-Erkenntnisse basierend auf der Domain-Reputation wurden hinzugefügt.	Es wurden 4 neue Arten von Erkenntnistypen hinzugefügt, die auf der Domain-Reputation basieren. Impact:EC2/AbusedDomainRequest.Reputation , Impact:EC2/BitcoinDomainRequest.Reputation, Impact:EC2/MaliciousDomainRequest.Reputation. Außerdem wurde eine neue EC2-Erkenntnis für C&CActivity hinzugefügt. Impact:EC2/SuspiciousDomainRequest.Reputation	27. Januar 2021

Es wurden 4 neue Erkenntnistypen hinzugefügt.	Es wurden 3 neue S3-MaliciousIPCaller-Erkenntnisse hinzugefügt. Discovery:S3/MaliciousIPCaller, Exfiltration:S3/MaliciousIPCaller, Impact:S3/MaliciousIPCaller. Außerdem wurde eine neue EC2-Erkenntnis für C&CActivity hinzugefügt. Backdoor:EC2/C&CActivity.B	21. Dezember 2020
Der Erkenntnistyp UnauthorizedAccess:EC2/TorIPCaller wurde außer Betrieb genommen.	Der UnauthorizedAccess:EC2/TorIPCaller Ergebnistyp ist jetzt aus entfernt GuardDuty. Weitere Informationen.	1. Oktober 2020
Der Erkenntnistyp Impact:EC2/WinRmBruteForce wurde hinzugefügt.	Eine neue Auswirkungs-Erkenntnis Impact:EC2/WinRmBruteForce wurde hinzugefügt. Weitere Informationen.	17. September 2020
Der Erkenntnistyp Impact:EC2/PortSweep wurde hinzugefügt.	Eine neue Auswirkungs-Erkenntnis Impact:EC2/PortSweep wurde hinzugefügt. Weitere Informationen.	17. September 2020
GuardDuty ist jetzt in den Regionen Afrika (Kapstadt) und Europa (Mailand) verfügbar.	Afrika (Kapstadt) und Europa (Mailand) wurden zur Liste der AWS Regionen hinzugefügt, in denen GuardDuty es verfügbar ist. Weitere Informationen	31. Juli 2020

Es wurden neue Nutzungsdetails zur GuardDuty Kostenüberwachung hinzugefügt.	Sie können jetzt neue Metriken verwenden, um GuardDuty Nutzungskostendaten für Ihr Konto und die von Ihnen verwalteten Konten abzufragen. Eine neue Übersicht der Nutzungskosten ist in der Konsole unter verfügbar https://console.aws.amazon.com/guardduty/. Detailliertere Informationen können über die API abgerufen werden.	31. Juli 2020
Inhalt zum S3-Schutz durch Überwachung von S3-Datenereignissen in hinzugefügt GuardDuty.	GuardDuty S3 Protection ist jetzt durch die Überwachung von Ereignissen auf der S3-Datenebene als neue Datenquelle verfügbar. Bei neuen Konten wird dieses Feature automatisch aktiviert. Wenn Sie sie bereits verwenden, können GuardDuty Sie die neue Datenquelle für sich selbst oder Ihre Mitgliedskonten aktivieren.	31. Juli 2020
Es wurden 14 neue S3-Erkenntnisse hinzugefügt.	14 neue S3-Erkenntnistypen wurden für Quellen der S3-Steuerebene und -Datenebene hinzugefügt.	31. Juli 2020

Zusätzliche Unterstützung für S3-Erkenntnisse hinzugefügt und zwei vorhandene Erkenntnistyp-Namen geändert.	GuardDuty Die Ergebnisse enthalten jetzt mehr Details zu Ergebnissen, die S3-Buckets betreffen. Bestehende Erkenntnistypen, die sich auf die S3-Aktivität bezogen, wurden umbenannt: Policy:IAMUser/S3BlockPublicAccessDisabled wurde zu Policy:S3/BucketBlockPublicAccessDisabled geändert. Stealth:IAMUser/S3ServerAccessLoggingDisabled wurde geändert zu Stealth:S3/ServerAccessLoggingDisabled.	28. Mai 2020
Inhalt für die AWS Organizations Integration hinzugefügt.	GuardDuty lässt sich jetzt in AWS Organizations delegierte Administratoren integrieren, sodass Sie GuardDuty Konten innerhalb Ihrer Organisation verwalten können. Wenn Sie einen delegierten Administrator als GuardDuty Administratorkonto einrichten, können Sie automatisch aktivieren, dass jedes Organisationsmitglied über das Konto GuardDuty für delegierte Administratoren verwaltet wird. Sie können das Konto auch automatisch für neue AWS Organizations Mitglieder aktivieren GuardDuty . Weitere Informationen.	20. April 2020

Inhalt für das Feature zum Export von Erkenntnissen hinzugefügt.	Inhalt hinzugefügt, der die Funktion „Ergebnisse exportieren“ von beschreibt GuardDuty.	14. November 2019
Der Erkenntnistyp UnauthorizedAccess:EC2/MetadataDNSRebind wurde hinzugefügt.	Eine neue unautorisierte Erkenntnis UnauthorizedAccess:EC2/MetadataDNSRebind wurde hinzugefügt. Weitere Informationen.	10. Oktober 2019
Der Erkenntnistyp Stealth:IAMUser/S3ServerAccessLoggingDisabled wurde hinzugefügt.	Eine neue Stealth-Erkenntnis Stealth:IAMUser/S3ServerAccessLoggingDisabled wurde hinzugefügt. Weitere Informationen.	10. Oktober 2019
Der Erkenntnistyp Policy:IAMUser/S3BlockPublicAccessDisabled wurde hinzugefügt.	Eine neue Richtlinien-Erkenntnis Policy:IAMUser/S3BlockPublicAccessDisabled wurde hinzugefügt. Weitere Informationen.	10. Oktober 2019
Der Erkenntnistyp Backdoor:EC2/XORDDOS wurde außer Betrieb genommen.	Der Backdoor:EC2/XORDDOS Ergebnistyp ist jetzt entfernt GuardDuty. Erfahren Sie mehr	12. Juni 2019
Der Erkenntnistyp Privilege Escalation wurde hinzugefügt.	Der PrivilegeEscalation-Erkenntnistyp erkennt, wenn Benutzer versuchen, ihren Konten eskalierte Berechtigungen mit weniger Einschränkungen zuzuweisen. Weitere Informationen	14. Mai 2019

GuardDuty ist jetzt in der Region Europa (Stockholm) verfügbar.	Europa (Stockholm) zur Liste der AWS Regionen hinzugefügt, in denen GuardDuty es verfügbar ist. Weitere Informationen	9. Mai 2019
Ein neuer Erkenntnistyp Recon:EC2/PortProbeEMRUnprotectedPort wurde hinzugefügt.	Dieses Ergebnis informiert Sie darüber, dass ein EMR-related sensibler Port auf einer EC2-Instance nicht blockiert ist und aktiv getestet wird. Weitere Informationen	8. Mai 2019
Es wurden 5 neue Erkenntnistypen hinzugefügt, die erkennen, wenn Ihre EC2-Instances für Denial-of-Service (DoS)-Angriffe genutzt werden.	Diese Ergebnisse informieren Sie von EC2-Instances in Ihrer Umgebung, deren Verhalten darauf hinweist, dass sie möglicherweise für Denial-of-Service (DoS)-Angriffe genutzt werden. Weitere Informationen	8. März 2019
Ein neuer Erkenntnistyp Policy:IAMUser/RootCredentialUsage wurde hinzugefügt.	Policy:IAMUser/RootCredentialUsageDie Suche nach dem Typ informiert Sie darüber, dass Ihre Root-Benutzeranmeldedaten für programmatische Anfragen an Dienste verwendet AWS-Konto werden. AWS Weitere Informationen	24. Januar 2019

Der UnauthorizedAccess :IAMUser/UnusualASNCaller-Erkenntnistyp wurde außer Betrieb genommen	Der UnauthorizedAccess :IAMUser/UnusualASNCaller-Erkenntnistyp wurde außer Betrieb genommen. Sie werden nun über Aktivitäten informiert, die von ungewöhnlichen Netzwerken über andere aktive GuardDuty Suchtypen aufgerufen wurden. Der generierte Ergebnistyp basiert auf der Kategorie der API, die von einem unüblichen Netzwerk aufgerufen wurde. Weitere Informationen	21. Dezember 2018
Zwei neue Erkenntnistypen wurden hinzugefügt: PenTest:IAMUser/ParrotLinux und PenTest:IAMUser/PentooLinux	Der PenTest:IAMUser/ParrotLinux-Erkenntnistyp informiert Sie darüber, dass ein Computer, auf dem Parrot Security Linux ausgeführt wird, API-Aufrufe mit Anmeldeinformationen durchführt, die zu Ihrem AWS -Konto gehören. Der PenTest:IAMUser/PentooLinux-Erkenntnistyp informiert Sie darüber, dass ein Computer, auf dem Pentoo Linux ausgeführt wird, API-Aufrufe mit Anmeldeinformationen durchführt, die zu Ihrem AWS -Konto gehören. Weitere Informationen	21. Dezember 2018

Unterstützung für das SNS-Thema mit GuardDuty Ankündigungen von Amazon wurde hinzugefügt	Sie können jetzt das SNS-Thema für GuardDuty Ankündigungen abonnieren, um Benachrichtigungen über neu veröffentlichte Suchtypen, Aktualisierungen der vorhandenen Suchtypen und andere Funktionsänderungen zu erhalten. Benachrichtigungen sind in allen Formaten verfügbar, die Amazon SNS unterstützt. Weitere Informationen	21. November 2018
Zwei neue Erkenntnistypen wurden hinzugefügt: UnauthorizedAccess:EC2/TorClient und UnauthorizedAccess:EC2/TorRelay	UnauthorizedAccess:EC2/TorClientFinding Type informiert dich darüber, dass eine EC2-Instance in deiner AWS Umgebung Verbindungen zu einem Tor Guard- oder Authority-Knoten herstellt. UnauthorizedAccess:EC2/TorRelayWenn Sie den Typ finden, werden Sie darüber informiert, dass eine EC2-Instance in Ihrer AWS Umgebung Verbindungen zu einem Tor-Netzwerk herstellt, und zwar auf eine Weise, die darauf hindeutet, dass sie als Tor-Relay fungiert. Weitere Informationen	16. November 2018

Ein neuer Erkenntnistyp CryptoCurrency:EC2/BitcoinTool.B wurde hinzugefügt.	Dieses Ergebnis informiert dich darüber, dass eine EC2-Instance in deiner AWS Umgebung einen Domainnamen abfragt, der mit Bitcoin oder einer anderen kryptowährungsbezogenen Aktivität verknüpft ist. Weitere Informationen	9. November 2018
Unterstützung für die Aktualisierung der Häufigkeit von Benachrichtigungen hinzugefügt, die an Ereignisse gesendet werden CloudWatch	Sie können jetzt die Häufigkeit der an CloudWatch Events gesendeten Benachrichtigungen für das spätere Auftreten vorhandener Ergebnisse aktualisieren. Mögliche Werte sind 15 Minuten, 1 Stunde oder standardmäßig 6 Stunden. Weitere Informationen	9. Oktober 2018
Zusätzliche Unterstützung für Regionen hinzugefügt	Unterstützung für Regionen für AWS GovCloud (US-West) hinzugefügt. Erfahre mehr	25. Juli 2018
Unterstützung für CloudFormation StackSets in hinzugefügt GuardDuty	Sie können die GuardDuty Vorlage „Amazon aktivieren“ verwenden, um sie GuardDuty gleichzeitig in mehreren Konten zu aktivieren. Weitere Informationen	25. Juni 2018

Unterstützung für Regeln zur GuardDuty automatischen Archivierung hinzugefügt	Kunden können jetzt granulare Regeln für die automatische Archivierung erstellen, um Ergebnisse zu unterdrücken. Ergebnisse, die einer Regel für die automatische Archivierung entsprechen, GuardDuty werden automatisch als archiviert markiert. Auf diese Weise können Kunden die Einstellungen GuardDuty weiter anpassen, sodass nur relevante Ergebnisse in der Tabelle mit den aktuellen Ergebnissen angezeigt werden. Weitere Informationen	4. Mai 2018
GuardDuty ist in der Region Europa (Paris) verfügbar	GuardDuty ist jetzt in Europa (Paris) verfügbar, sodass Sie die kontinuierliche Sicherheitsüberwachung und Bedrohungserkennung in dieser Region ausweiten können. Weitere Informationen	29. März 2018
Das Erstellen von GuardDuty Administratorkonten und Mitgliedskonten über CloudFormation wird jetzt unterstützt.	Weitere Informationen erhalten Sie unter `AWS::GuardDuty::master` und `AWS::GuardDuty::member`.	6. März 2018
Neun neue CloudTrail-based Anomalieerkennungen wurden hinzugefügt.	Diese neuen Suchtypen werden automatisch GuardDuty in allen unterstützten Regionen aktiviert. Weitere Informationen	28. Februar 2018

Drei neue Bedrohungsinformationen wurden hinzugefügt (Erkennungstypen).	Diese neuen Suchtypen werden automatisch GuardDuty in allen unterstützten Regionen aktiviert. Weitere Informationen	5. Februar 2018
Erhöhung des Limits für GuardDuty Mitgliedskonten.	Mit dieser Version können Sie bis zu 1000 GuardDuty Mitgliedskonten pro AWS Konto hinzufügen (GuardDuty Administratorkonto). Weitere Informationen	25. Januar 2018
Änderungen beim Upload und bei der weiteren Verwaltung von Listen mit vertrauenswürdigen IP-Adressen und Bedrohungslisten für GuardDuty Administratorkonten und Mitgliedskonten.	Mit dieser Version können Benutzer mit GuardDuty Administratorkonten vertrauenswürdige IP-Listen und Bedrohungslisten hochladen und verwalten. Benutzer von GuardDuty Mitgliedskonten können keine Listen hochladen und verwalten. Vertrauenswürdige IP-Listen und Bedrohungslisten, die vom Administratorkonto hochgeladen werden, beeinträchtigen die GuardDuty Funktionalität der Mitgliedskonten. Weitere Informationen	25. Januar 2018

Frühere Aktualisierungen

Änderungen	Beschreibung	Date
Erste Veröffentlichung	Erste Veröffentlichung des GuardDuty Amazon-Be nutzerhandbuchs.	28. November 2017

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.